(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開2000-293439

（Ｐ２０００－２９３４３９Ａ）

(43)公開日　平成12年10月20日(2000.10.20)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｂ	5B017
15/00	３３０	15/00	３３０Ｄ	5B085

審査請求　未請求　請求項の数11　ＯＬ（全 29 頁）

(21)出願番号　特願平11-99482

(22)出願日　平成11年4月6日(1999.4.6)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中4丁目1番1号

(72)発明者　畠山　卓久
神奈川県川崎市中原区上小田中4丁目1番1号　富士通株式会社内

(72)発明者　吉岡　誠
神奈川県川崎市中原区上小田中4丁目1番1号　富士通株式会社内

(74)代理人　100089118
弁理士　酒井　宏明

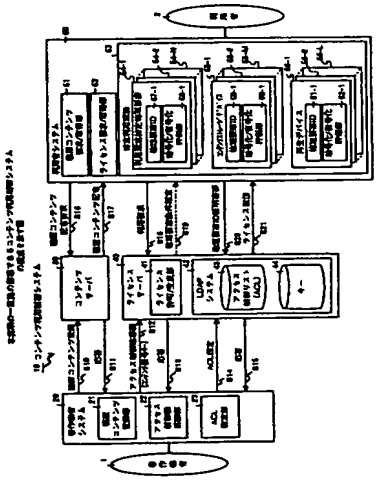
最終頁に続く

(54)【発明の名称】コンテンツ利用制御システム、コンテンツ利用装置およびその利用方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体

(57)【要約】

【課題】　情報提供権限者がコンテンツ利用制御を柔軟に行うことができるとともに、コンテンツの不正利用を精度高く防止することができる。

【解決手段】　著作権者システム２０とコンテンツサーバ３０とライセンスサーバ４０と利用者システム５０とを有し、著作権者システム２０のＡＣＬ設定部２３は、利用者システム５０で使用するメディアを含む複数の物理要素のＩＤおよび利用者ＩＤに基づいてコンテンツに対する複数の部分利用許可条件をさらに論理和および論理積の組み合わせによって構造化表現した利用許可条件ＡＣＬとして設定し、アクセス制御リスト４３に格納する。ライセンスサーバ４０は、このアクセス制御リスト４３を用いて利用者２によるコンテンツの利用を制御するが、このアクセス制御リストには、コンテンツの利用状況に応じた条件、たとえば操作可能回数最大値や課金条件等の会計条件も設定することができる。



1

【特許請求の範囲】

【請求項１】　コンテンツの作成者である情報作成者および該情報作成者によって許諾された者を含む情報提供権限者によって提供される該コンテンツの利用制御を行うコンテンツ利用制御システムにおいて、

前記コンテンツを利用者が利用する利用者手段と、

前記利用者手段内で使用するメディアを含む当該利用者手段の物理要素に関する識別情報および前記利用者に関する識別情報に基づいた前記コンテンツに対する複数の部分利用許可条件をさらに論理和および論理積の組み合わせによって構造化表現した利用許可条件として設定する設定手段と、

前記設定手段によって設定された利用許可条件をもとに前記利用者手段による前記コンテンツの利用を制御する利用制御手段と、

を備えたことを特徴とするコンテンツ利用制御システム。

【請求項２】　前記設定手段が設定する部分利用許可条件は、前記利用者手段および前記利用者の利用状況に応じて変化するカテゴリーに対する条件である会計条件を含むことを特徴とする請求項１に記載のコンテンツ利用制御システム。

【請求項３】　前記利用制御手段は、前記利用者手段からのコンテンツ利用要求を受けて、前記利用許可条件および前記コンテンツの復号キーを前記利用者手段内で使用するメディアを含む当該利用者手段の複数の物理要素に関する識別情報によって暗号化した許諾情報を生成する生成手段を備え、

前記利用者手段は、前記コンテンツ利用要求に応じて送られる前記許諾情報を当該利用者手段による物理要素の識別情報をもとに復号し、前記利用許可条件を満足する場合に前記コンテンツの復号キーを用いて前記暗号化されたコンテンツの復号を行うことを特徴とする請求項１または２に記載のコンテンツ利用制御システム。

【請求項４】　前記生成手段は、前記利用許可条件内の部分利用許可条件間が論理積で記述されている場合には、当該部分利用許可条件に対応する物理要素の識別情報による暗号化を多重化して行うことを特徴とする請求項３に記載のコンテンツ利用制御システム。

【請求項５】　前記物理要素は、他の物理要素に包含された物理要素を含むことを特徴とする請求項１～４のいずれか一つに記載のコンテンツ利用制御システム。

【請求項６】　開放ネットワーク上に、前記情報提供権限者手段によって暗号化したコンテンツを保持し、前記利用者手段からのコンテンツ配布要求を受け付けて前記暗号化したコンテンツを当該利用者手段に送付するコンテンツサーバをさらに備えたことを特徴とする請求項１～５のいずれか一つに記載のコンテンツ利用制御システム。

【請求項７】　コンテンツの作成者である情報作成者および該情報作成者によって許諾された者を含む情報提供権限者によって提供される該コンテンツの利用制御を行うコンテンツ利用制御システムにおいて、

2

コンテンツの利用要求を行い、当該コンテンツ利用要求に応じて送られる許諾要求を当該手段の物理要素の識別情報をもとに復号して得られた利用許可条件を満足する場合に前記コンテンツの復号キーを用いて暗号化されたコンテンツの復号を行う利用者手段と、

前記利用者手段内で使用するメディアを含む当該利用者手段の物理要素に関する識別情報および前記利用者に関する識別情報に基づいた前記コンテンツに対する複数の部分利用許可条件をさらに論理和および論理積の組み合わせによって構造化表現した利用許可条件を予め設定する設定手段と、

前記設定手段によって設定された利用許可条件を格納する条件格納手段と、

前記コンテンツの復号キーを保持する保持手段と、

前記利用者手段からのコンテンツの利用要求を受け付けて当該利用者手段に対応する利用許可条件および前記コンテンツの復号キーを抽出する抽出手段と、

前記利用者手段から送付された物理要素の識別情報をもとに前記利用許可条件および前記コンテンツの復号キーを暗号化した許諾情報を生成して当該利用者手段に送出する生成手段と、

を備えたことを特徴とするコンテンツ利用制御システム。

【請求項８】　ネットワークに接続して利用者がコンテンツの利用を行うコンテンツ利用装置において、

コンテンツの利用要求に応じて、コンテンツの管理を行うコンテンツ管理装置に、当該コンテンツ利用装置の物理要素に関する識別情報および利用者に関する識別情報を送信する要求手段と、

前記コンテンツの利用要求に対応してコンテンツ管理装置によって送信される許諾情報から、当該コンテンツ利用装置の物理要素に関する識別情報をもとに復号して利用許可条件およびコンテンツの復号キーを求める手段と、

前記求めた利用許可条件を判定し許可される場合に前記求めた復号キーを用いてコンテンツの復号を行う手段と、

を備えたことを特徴とするコンテンツ利用装置。

【請求項９】　ネットワークに接続して利用者がコンテンツの利用を行うコンテンツ利用装置のコンピュータで実行させるプログラムを格納したコンピュータ読み取り可能な記録媒体であって、

コンテンツの利用要求に応じて、コンテンツの管理を行うコンテンツ管理装置に、当該コンテンツ利用装置の物理要素に関する識別情報および利用者に関する識別情報を送信する要求工程と、

前記コンテンツの利用要求に対応してコンテンツ管理装

置によって送信される許諾情報から、当該コンテンツ利用装置の物理要素に関する識別情報をもとに復号して利用許可条件およびコンテンツの復号キーを求める工程と、
前記求めた利用許可条件を判定し許可される場合に前記求めた復号キーを用いてコンテンツの復号を行う手段と、
を動作させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項１０】　利用者がコンテンツの利用を行うコンテンツ利用装置において、
前記コンテンツの利用要求に対応して、コンテンツの許諾情報から、当該コンテンツ利用装置の物理要素に関する識別情報をもとに復号して利用許可条件およびコンテンツの復号キーを求める手段と、
前記求めた利用許可条件を判定し許可される場合に、前記求めた復号キーを用いてコンテンツの復号を行う手段と、
を備えたことを特徴とするコンテンツ利用装置。

【請求項１１】　利用者がコンテンツの利用を行うコンテンツ利用装置のコンピュータで実行させるプログラムを格納したコンピュータ読み取り可能な記録媒体であって、
前記コンテンツの利用要求に対応して、コンテンツの許諾情報から、当該コンテンツ利用装置の物理要素に関する識別情報をもとに復号して利用許可条件およびコンテンツの復号キーを求める工程と、
前記求めた利用許可条件を判定し許可される場合に、前記求めた復号キーを用いてコンテンツの復号を行う工程と、
を動作させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、著作権者等の情報提供権限者が開放ネットワークを介して提供するコンテンツの利用を制御するコンテンツ利用制御システム、コンテンツ利用装置およびその利用方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体に関するものである。

【０００２】貨幣の役割は、その貨幣という物質としての性質によって、公平な報酬を人々に提供する。貨幣というオブジェクトは、単なる口約束的共有概念ではなく、物理的に存在し、携帯でき、さらに発行元以外による偽造が困難であることが必須要件であった。物理的に存在し、携帯できることによって、その価値の利用者同士で公平に確認することができ、偽造の困難性によって、その公平な確認の契機を公平なる貨幣の発行元がコントロールすることができた。しかし、近年の工業技術の発展によって、今や貨幣の偽造困難性が崩壊する日が近い。貨幣に代わる新たな価値確認オブジェクトが必要になっている。そのオブジェクトはやはり、まず物理的に存在し、携帯でき、偽造困難である必要がある。さらにそのオブジェクトは発行元がアクセスコントロールできる必要がある。

【０００３】このセキュリティ強化面からの要求に加え、情報流通の多様化と大容量化、高速化の側面から「超流通」の実現の要求も高まっている。この「超流通」を実現した環境は、つぎの条件を満足する。すなわち、（１）情報利用者は、デジタル情報をほぼ無料で入手できること、（２）情報提供者は、その情報の利用を許可する条件（課金、改変利用条件など）を指定し、利用者の合意した条件を強制することができること、（３）このサービスを利用するに当たって、必要な情報利用者の追加操作は「アクセス条件の確認」程度であること、である。

【０００４】こうした超流通のアクセス制御を正確かつ、安全に実行可能なシステムは、ライセンス料などの著作権料徴収の不公平の是正にも寄与することが期待できる。現行システムでは、著作物が相当数売れないと提供者は利益を上げられないが、正確に著作権者の手に渡るようにシステムを構築できることが望まれる。また、専門家的芸術家から、部品としての創作を提供するデザイナーに至るまで、各人のサービス料に見合う報酬が公平に分配されることが望まれる。

【０００５】

【従来の技術】従来、著作物等のコンテンツに対するアクセスを分散システム環境、特に開放ネットワーク上において制御する場合、コンテンツの利用者からのアクセスが可能なサーバにコンテンツを格納し、このサーバに対するアクセスを制御することによって、コンテンツの利用を制御していた。ここで、コンテンツとは、単一の記憶装置媒体に記録可能なビット列の集合としての構造をもつデジタルコンテンツであり、文書テキスト、画像、動画、プログラムソフトウェア等を含む。

【０００６】たとえば、図１７は、従来のアクセス制御モデルを示す図である。図１７において、コンテンツ２０４は、アクセス制御機能２０３を介してのみ、利用者２０５からのコンテンツ操作を可能としている。また、著作権者２００は、コンテンツ２０４をアクセス制御機能２０３で保護された、たとえばサーバに登録するのみで、著作権者２００以外の者、たとえばこのサーバを管理する管理者によってアクセス制御機能２０３に対するアクセス制御操作がなされていた。

【０００７】すなわち、図１８に示すようにコンテンツを保持するサーバシステム２１２は、管理者２０１によって管理運用されるサーバ運用者システム２１１によって管理され、サーバ運用者システム２１１は、サーバシステム２１２に対して著作権者および利用者登録を行い、またこのためのディレクトリ生成を行い、さらに

は、著作権者によるアクセス制御を許可することも行う。著作権者システム２１０は、著作権者の著作物のコンテンツをサーバシステム２１２に保存させ、アクセス制御条件（ＡＣＬ）をサーバシステム２１２に対して設定する。この場合、著作権者は、サーバシステム２１２に対してアクセス制御の許可を得なければならない。一方、利用者システム２１３は、コンテンツの利用に際して、コンテンツ送信要求をサーバシステム２１２に対して行い、ＡＣＬを満足する場合には、サーバシステム２１２内に保存されていたコンテンツを取得する。

【０００８】しかし、コンテンツの利用者にすべての権限が与えられ、移動やコピー（複製）によって利用者が変わると、移動あるいはコピー先のコンテンツに対しては、もとの著作権者の権限はまったく働かない。また、コンテンツオブジェクトを保存するサーバ管理者と著作権者の間では、オブジェクトに対するアクセス許諾強制のあり方も明確ではなく、たとえばサーバ管理者が著作権者に断りなく、アクセス権を変更可能なことが当然のこととされていた。

【０００９】一方、近年の記憶媒体等の低価格化等によって分散システム環境が促進され、ネットワークのトラフィックが集中することなく、コンテンツを複数のサーバにキャッシュして分散できるようになり、コンテンツオブジェクトに対するアクセスを高速に行うことができるようになった。従って、図１７に示すようなアクセス制御モデルは、利用者２０５によるコンテンツ操作への入り口のみに対して強固なアクセス制御機能を構築すればよいが、上述した分散システム環境下では、全方向的なアクセス制御あるいはセキュリティ保護を行う必要があった。

【００１０】そこで、図１９に示すようなアクセス制御モデルが考えられた。このアクセス制御モデルでは、著作権者２００が従来のセキュリティ技術で保護が可能な領域である著作権者保護領域と、あらゆる外部からの攻撃を受容する開放領域と、ハード／ソフトの改ざんの保護とデジタルデータ複製防止処理が施される秘匿保護領域とに分離される。秘匿保護領域は、全方位的なアクセス制御機能２２１によって保護し、このアクセス制御機能２２１内にコンテンツ２２２が保存される。

【００１１】このコンテンツに対して、著作権者２００は、コンテンツ２２２の登録とともに、アクセス制御機能２２１に対するアクセス制御操作も可能としている。利用者２０５は、開放領域から、アクセス制御機能２２１を介してコンテンツ２２２を取得することになる。なお、領域間保護インターフェース２２０は、著作権者保護領域と開放領域との間の保護を行うインターフェースである。

【００１２】この図１９に示す分散システム環境下におけるアクセス制御モデルの具体化は、米国特許５３３９４３３号公報に記載されており、また、特開平９－１３４３１１号公報、米国特許５３９２３５１号公報、米国特許５５５５３０４号公報、および米国特許５７９６８２４号公報には、利用者の機器をチェックしてコンテンツの不正利用を防止する技術が記載されている。以下、これらの公報を参照して従来のコンテンツ利用制御システムについて説明する。

【００１３】図２０は、従来のコンテンツ利用制御システムのコンテンツ配布モデルを示す図である。図２０において、復号保護領域と再生保護領域とは、図１８に示す秘匿保護領域に相当し、復号保護領域は、ハード／ソフトの改ざんの保護と出力データの複製防止保護の領域であり、再生保護領域は、デジタル復号データの複製防止の領域である。利用環境特定物理要素（ＰＣＳＵＥ）２３５－１～２３５－Ｎは、コンテンツの利用環境を特定する物理要素であり、具体的には、ＣＰＵ、周辺装置、リムーバブルな記憶媒体、ＩＣカード等である。

【００１４】復号保護領域では、ＰＣＳＵＥ２３５－１～２３５－Ｎに対応する物理要素ＩＤの証明書２３６－１～２３６－Ｎをもとに、著作権者２００によって暗号化されたコンテンツ２３３の複製であって開放領域のサーバに存在するコンテンツ２３４を復号し、再生保護領域を介して、この複合されたコンテンツが利用者に利用される。従って、コンテンツは、物理要素ＩＤに対応したキーで暗号化され（コンテンツ２３３）、このコンテンツ２３３に対応するコンテンツ２３４を復号するためには、各物理要素ＩＤまたはそれに対応した秘密のキーが必要となる。

【００１５】ここで、コンテンツ配布モデルには、暗号化されたコンテンツを復号するために用いられるライセンスを、暗号化されたコンテンツと同時に配布するライセンス同時モデルと、暗号化されたコンテンツをサーバのキャッシュに保存し、ライセンスとは別のタイミングで取得するコンテンツキャッシュ可能型モデルとがある。図２１は、このコンテンツキャッシュ可能型モデルを示す図である。

【００１６】図２１において、まず著作者２００は、著作権者保護領域で、コンテンツを生成し、このコンテンツを暗号化し、その後、複製して開放領域のサーバ等にキャッシュされる。一方、ＰＣＳＵＥ２３５－１～２３５－Ｎの物理要素ＩＤを暗号化した証明書２４１－１～２４１－Ｎは、暗号化された状態で著作権者保護領域に出力され、ＰＣＳＵＥ２３５－１～２３５－Ｎに対応する利用者物理オブジェクトクラスから秘密キーＫｐを取り出し、この秘密キーＫｐと証明書２４１－１～２４１－Ｎとから物理要素ＩＤ２４３－１～２４３－Ｎを復号し、この物理要素ＩＤ２４３－１～２４３－Ｎによってコンテンツ復号キーＫｃを暗号化し、秘密保護領域に出力する。

【００１７】秘密保護領域では、暗号化されたコンテンツ復号キーＫｃを物理要素ＩＤ２４２－１～２４２－Ｎ

で復号し、コンテンツ復号キーＫｃを得る。このコンテンツ復号キーＫｃを用いて開放領域から取得される、暗号化されたコンテンツ２３４を復号し、コンテンツ２４４として利用者２０５に利用させる。

【００１８】図２２は、図２１に示すコンテンツキャッシュ可能型モデルに対応するコンテンツ利用制御システムの概要構成を示すブロック図である。図２２において、著作権者システム２５０は、著作権者保護領域に存在し、コンテンツサーバ２５１は、開放領域に存在し、ライセンスサーバ２５２および利用者システム２５３は、秘匿保護領域に存在する。著作権者システム２５０は、作成したコンテンツを暗号化し、この暗号化した秘匿コンテンツをコンテンツサーバ２５１に保存しておく。

【００１９】また、コンテンツ復号キーＫｃをライセンスサーバ２５２に送信して、アクセス制御権の委譲をライセンスサーバ２５２に対して行う。さらに、アクセス制御リスト（ＡＣＬ）設定を行う。利用者システム２５３は、コンテンツを利用することを示す利用要求をライセンスサーバ２５２に送信し、このとき、物理要素ＩＤの証明群が添付されていない場合には、ライセンスサーバ２５２の物理要素条件指定によって物理要素ＩＤの証明群を取得し、ライセンスサーバ２５２に送出する。

【００２０】ライセンスサーバ２５２は、図２１に示したように、利用者の物理オブジェクトクラスの秘密キーＫｐを取得して物理要素ＩＤ証明群を復号し、復号した物理要素ＩＤによって暗号化されたコンテンツ復号キーＫｃがライセンスＬとして利用者システム２５３に送出される。これによって、利用者システム２５３の物理要素ＩＤが一致すれば、復号が行われ、この復号されたコンテンツ復号キーＫｃを用いて秘匿コンテンツを復号することができる。

【００２１】なお、秘密コンテンツはコンテンツサーバ２５１に保存されているので、利用者システム２５３は、別途コンテンツサーバ２５１に秘密コンテンツ配布要求を行って、コンテンツサーバ２５１から秘密コンテンツの配布を受ける必要がある。

【００２２】一方、図２３は、コンテンツ同時配布型モデルを実現するコンテンツ利用制御システムの概要構成ブロック図を示している。図２３では、コンテンツサーバ２５１が存在せず、ライセンス送信と同時に利用者システム２５３に送付されることになる。図２２に示すように、コンテンツサーバ２５１を介して秘密コンテンツを取得する場合、秘密コンテンツは予め時間的に利用者システム２５３に近いサーバまで運ばれているので、利用者システム２５３は、コンテンツが必要な時に利用要求をすればよい。

【００２３】また、コンテンツ同時配布型モデルに比較してコンテンツの流通経路の適切な選択が可能となり、利用者にとっては、コンテンツ取得に際して応答時間の短縮が期待できる。また、コンテンツキャッシュ可能型モデルでは、コンテンツを、ライセンスの提供とは別に、ＲＯＭ媒体ベース、放送、Ｐｒｏｘｙサーバによるキャッシュ等によって、予め配布しておくことが可能であり、利点が多い。

【００２４】

【発明が解決しようとする課題】しかしながら、上述した従来のコンテンツ利用制御システムでは、利用者システムに固有の物理要素ＩＤに一致する装置であれば、基本的に秘匿コンテンツを復号でき、このコンテンツを利用することができるが、この物理要素ＩＤのみによってライセンス（利用許可条件）を生成しているので、たとえば、著作権者の意思で決定されるコンテンツの読み出し回数を制限する条件を付加したり、時間制限を設けたり、課金条件を設定したりすることができず、柔軟なコンテンツ利用制御ができないという問題点があった。

【００２５】また、利用環境特定物理要素は、常に単純な構成となってるとは限らず、複雑な構成をもった機器である場合には、その機器のうちの特定の機器あるいは部品が不正である場合もあり、このような場合に、単に大きな構成の機器である利用環境特定物理要素によって利用許可条件を生成しても、不正を見逃してしまうことなりセキュリティが低下するという問題点があった。

【００２６】この発明は上記に鑑みてなされたもので、著作権者等の情報作成者に許諾された者を含む情報提供権限者がコンテンツ利用制御を柔軟に行うことができるとともに、コンテンツの不正利用を精度高く防止することができるコンテンツ利用制御システム、コンテンツ利用装置およびその利用方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体を提供することを目的とする。

【００２７】

【課題を解決するための手段】上記目的を達成するため、請求項１にかかる発明は、コンテンツの作成者である情報作成者および該情報作成者によって許諾された者を含む情報提供権限者によって提供される該コンテンツの利用制御を行うコンテンツ利用制御システムにおいて、前記コンテンツを利用者が利用する利用者手段（図１の５０）と、前記利用者手段内で使用するメディアを含む当該利用者手段の物理要素に関する識別情報および前記利用者に関する識別情報に基づいた前記コンテンツに対する複数の部分利用許可条件をさらに論理和および論理積の組み合わせによって構造化表現した利用許可条件として設定する設定手段（図１の２３）と、前記設定手段によって設定された利用許可条件をもとに前記利用者手段による前記コンテンツの利用を制御する利用制御手段（図１の４０）と、を備えたことを特徴とする。

【００２８】この請求項１にかかる発明によれば、設定手段が、前記利用者手段内で使用するメディアを含む当該利用者手段の物理要素に関する識別情報および前記利

用者に関する識別情報に基づいた前記コンテンツに対する複数の部分利用許可条件をさらに論理和および論理積の組み合わせによって構造化表現した利用許可条件として設定し、前記利用制御手段は、前記設定手段によって設定された利用許可条件をもとに前記利用者手段による前記コンテンツの利用を制御し、利用許可条件に基づいた柔軟な利用制御を可能とする。

【００２９】また、請求項２にかかる発明は、請求項１に記載のコンテンツ利用制御システムにおいて、前記設定手段が設定する部分利用許可条件は、前記利用者手段および前記利用者の利用状況に応じて変化するカテゴリーに対する条件である会計条件（図３の会計条件値に相当）を含むことを特徴とする。

【００３０】この請求項２にかかる発明によれば、設定手段よって設定される部分利用許可条件は、前記利用者手段および前記利用者の利用状況に応じて変化するカテゴリーに対する条件である会計条件を含むようにし、一層利用者に対する利用制御を細かに行うことができる。

【００３１】また、請求項３にかかる発明は、請求項１または２に記載のコンテンツ利用制御システムにおいて、前記利用制御手段（図１の４０）は、前記利用者手段（図１の５０）からのコンテンツ利用要求（図１のＳ１８）を受けて、前記利用許可条件および前記コンテンツの復号キーを前記利用者手段内で使用するメディアを含む当該利用者手段の複数の物理要素に関する識別情報によって暗号化した許諾情報を生成する生成手段（図１の４１）を備え、前記利用者手段は、前記コンテンツ利用要求に応じて送られる前記許諾情報を当該利用者手段による物理要素の識別情報をもとに復号し、前記利用許可条件を満足する場合に前記コンテンツの復号キーを用いて前記暗号化されたコンテンツの復号を行うことを特徴とする。

【００３２】この請求項３にかかる発明によれば、生成手段が、前記利用者手段からのコンテンツ利用要求を受けて、前記利用許可条件および前記コンテンツの復号キーを前記利用者手段内で使用するメディアを含む当該利用者手段の複数の物理要素に関する識別情報によって暗号化した許諾情報を生成し、前記利用者手段は、前記コンテンツ利用要求に応じて送られる前記許諾情報を当該利用者手段による物理要素の識別情報をもとに復号し、前記利用許可条件を満足する場合に前記コンテンツの復号キーを用いて前記暗号化されたコンテンツの復号を行う。

【００３３】また、請求項４にかかる発明は、請求項３のコンテンツ利用制御システムにおいて、前記生成手段（図１の４１）は、前記利用許可条件内の部分利用許可条件間が論理積で記述されている場合には、当該部分利用許可条件に対応する物理要素の識別情報による暗号化を多重化して（数１および数２に相当）行うことを特徴とする。

【００３４】この請求項４にかかる発明によれば、利用許可条件内の部分利用許可条件間が論理積で記述されている場合には、当該部分利用許可条件に対応する物理要素の識別情報による暗号化を多重化して行い、一部の物理要素に対する攻撃成功によるコンテンツ復号キーの盗難の危険性を分散することができる。

【００３５】また、請求項５にかかる発明は、請求項１～４に記載のコンテンツ利用制御システムにおいて、前記物理要素は、他の物理要素に包含された物理要素（図９の１３１～１３６）を含むことを特徴とする。

【００３６】この請求項５にかかる発明によれば、物理要素が包含関係にある物理要素であっても一つの物理要素として取り扱い、この一つの物理要素の不正も許さず、コンテンツ復号キーの盗難という危険性を分散することができる。

【００３７】また、請求項６にかかる発明は、請求項１～５に記載のコンテンツ利用制御システムにおいて、開放ネットワーク上に、前記情報提供権限者手段によって暗号化したコンテンツを保持し、前記利用者手段からのコンテンツ配布要求を受け付けて前記暗号化したコンテンツを当該利用者手段に送付するコンテンツサーバ（図１の３０）をさらに備えたことを特徴とする。

【００３８】この請求項６にかかる発明によれば、開放ネットワーク上に、前記情報提供権限者手段によって暗号化したコンテンツを保持し、前記利用者手段からのコンテンツ配布要求を受け付けて前記暗号化したコンテンツを当該利用者手段に送付するコンテンツサーバを有しているので、開放ネットワークを十分に活用して当該システムにおけるトラフィックの輻輳を防止して、迅速にコンテンツを獲得することができる。

【００３９】また、請求項７にかかる発明は、コンテンツの作成者である情報作成者および該情報作成者によって許諾された者を含む情報提供権限者によって提供される該コンテンツの利用制御を行うコンテンツ利用制御システムにおいて、コンテンツの利用要求を行い、当該コンテンツ利用要求に応じて送られる許諾要求を当該手段の物理要素の識別情報をもとに復号して得られた利用許可条件を満足する場合に前記コンテンツの復号キーを用いて暗号化されたコンテンツの復号を行う利用者手段（図１の５０）と、前記利用者手段内で使用するメディアを含む当該利用者手段の物理要素に関する識別情報および前記利用者に関する識別情報に基づいた前記コンテンツに対する複数の部分利用許可条件をさらに論理和および論理積の組み合わせによって構造化表現した利用許可条件を予め設定する設定手段（図１の２３）と、前記設定手段によって設定された利用許可条件を格納する条件格納手段（図１の４３）と、前記コンテンツの復号キーを保持する保持手段（図１の４４）と、前記利用者手段からのコンテンツの利用要求を受け付けて当該利用者手段に対応する利用許可条件および前記コンテンツの復

号キーを抽出する抽出手段（図４２）と、前記利用者手段から送付された物理要素の識別情報をもとに前記利用許可条件および前記コンテンツの復号キーを暗号化した許諾情報を生成して当該利用者手段に送出する生成手段（図１の４１）と、を備えたことを特徴とする。

【００４０】この請求項７にかかる発明によれば、設定手段が、利用者手段内で使用するメディアを含む当該利用者手段の物理要素に関する識別情報および前記利用者に関する識別情報に基づいた前記コンテンツに対する複数の部分利用許可条件をさらに論理和および論理積の組み合わせによって構造化表現した利用許可条件を前記利用制御手段内の条件格納手段に格納することによって予め設定するとともに、保持手段に前記コンテンツの復号キーを保持する。抽出手段は、前記利用者手段からのコンテンツの利用要求を受け付けて当該利用者手段に対応する利用許可条件および前記コンテンツの復号キーを抽出し、前記利用者手段から送付された物理要素の識別情報をもとに前記利用許可条件および前記コンテンツの復号キーを暗号化した許諾情報を生成して当該利用者手段に送出する。利用者手段は、前記コンテンツ利用要求に応じて送られる前記許諾情報を当該利用者手段による物理要素の識別情報をもとに復号し、前記利用許可条件を満足する場合に前記コンテンツの復号キーを用いて前記暗号化されたコンテンツの復号を行う。

【００４１】また、請求項８にかかる発明は、ネットワークに接続して利用者がコンテンツの利用を行うコンテンツ利用装置において、コンテンツの利用要求に応じて、コンテンツの管理を行うコンテンツ管理装置に、当該コンテンツ利用装置の物理要素に関する識別情報および利用者に関する識別情報を送信する要求手段（図１の５２）と、前記コンテンツの利用要求に対応してコンテンツ管理装置によって送信される許諾情報から、当該コンテンツ利用装置の物理要素に関する識別情報をもとに復号して利用許可条件およびコンテンツの復号キーを求める手段（図１の５８－１，６０－１，６２－１）と、前記求めた利用許可条件を判定し許可される場合に前記求めた復号キーを用いてコンテンツの復号を行う手段（図１の５１）と、を備えたことを特徴とする。

【００４２】この請求項８にかかる発明によれば、要求手段が、コンテンツの利用要求に応じて、コンテンツの管理を行うコンテンツ管理装置に、当該コンテンツ利用装置の物理要素に関する識別情報および利用者に関する識別情報を送信すると、その後、前記コンテンツの利用要求に対応してコンテンツ管理装置によって送信される許諾情報から、当該コンテンツ利用装置の物理要素に関する識別情報をもとに復号して利用許可条件およびコンテンツの復号キーを求め、前記求めた利用許可条件を判定し許可される場合に前記求めた復号キーを用いてコンテンツの復号を行うようにして、保護強度を高くしている。

【００４３】また、請求項９にかかる発明は、ネットワークに接続して利用者がコンテンツの利用を行うコンテンツ利用装置のコンピュータで実行させるプログラムを格納したコンピュータ読み取り可能な記録媒体であって、コンテンツの利用要求に応じて、コンテンツの管理を行うコンテンツ管理装置に、当該コンテンツ利用装置の物理要素に関する識別情報および利用者に関する識別情報を送信する要求工程（図１１のＳ５０１）と、前記コンテンツの利用要求に対応してコンテンツ管理装置によって送信される許諾情報から、当該コンテンツ利用装置の物理要素に関する識別情報をもとに復号して利用許可条件およびコンテンツの復号キーを求める工程（図１２のＳ６００，Ｓ６０１、図１３のＳ７００，Ｓ７０１）と、前記求めた利用許可条件を判定し許可される場合に前記求めた復号キーを用いてコンテンツの復号を行う工程（図１３のＳ７０４）と、を動作させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体である。

【００４４】この請求項９にかかる発明によれば、まず要求工程によって、コンテンツの利用要求に応じて、コンテンツの管理を行うコンテンツ管理装置に、当該コンテンツ利用装置の物理要素に関する識別情報および利用者に関する識別情報を送信し、その後、前記コンテンツの利用要求に対応してコンテンツ管理装置によって送信される許諾情報から、当該コンテンツ利用装置の物理要素に関する識別情報をもとに復号して利用許可条件およびコンテンツの復号キーを求め、その後、前記求めた利用許可条件を判定し許可される場合に前記求めた復号キーを用いてコンテンツの復号を行うようにして、保護強度を高くする。

【００４５】また、請求項１０にかかる発明は、利用者がコンテンツの利用を行うコンテンツ利用装置において、前記コンテンツの利用要求に対応して、コンテンツの許諾情報から、当該コンテンツ利用装置の物理要素に関する識別情報をもとに復号して利用許可条件およびコンテンツの復号キーを求める手段（図１の５８－１，６０－１，６２－１）と、前記求めた利用許可条件を判定し許可される場合に、前記求めた復号キーを用いてコンテンツの復号を行う手段（図１の５１）と、を備えたことを特徴とする。

【００４６】この請求項１０にかかる発明によれば、まず、コンテンツの利用要求に対応して、コンテンツの許諾情報から、当該コンテンツ利用装置の物理要素に関する識別情報をもとに復号して利用許可条件およびコンテンツの復号キーを求め、その後、前記求めた利用許可条件を判定し許可される場合に、前記求めた復号キーを用いてコンテンツの復号を行うようにして、保護強度を高くする。

【００４７】また、請求項１１にかかる発明は、利用者がコンテンツの利用を行うコンテンツ利用装置のコンピ

ュータで実行させるプログラムを格納したコンピュータ読み取り可能な記録媒体であって、前記コンテンツの利用要求に対応して、コンテンツの許諾情報から、当該コンテンツ利用装置の物理要素に関する識別情報をもとに復号して利用許可条件およびコンテンツの復号キーを求める工程（図１２のＳ６００，Ｓ６０１、図１３のＳ７００，Ｓ７０１）と、前記求めた利用許可条件を判定し許可される場合に、前記求めた復号キーを用いてコンテンツの復号を行う工程（図１３のＳ７０４）と、を動作させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体である。

【００４８】この請求項１１にかかる発明によれば、まず、前記コンテンツの利用要求に対応して、コンテンツの許諾情報から、当該コンテンツ利用装置の物理要素に関する識別情報をもとに復号して利用許可条件およびコンテンツの復号キーを求め、その後、前記求めた利用許可条件を判定し許可される場合に、前記求めた復号キーを用いてコンテンツの復号を行うようにして、保護強度を高くする。

【００４９】

【発明の実施の形態】以下に添付図面を参照して、本発明にかかるコンテンツ利用制御システム、コンテンツ利用装置およびその利用方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体の好適な実施の形態を説明する。

【００５０】図１は、本発明の一実施の形態であるコンテンツ利用制御システムの構成を示す図である。図１に示すコンテンツ利用制御システム１０は、著作権者１が作成した著作物のコンテンツを利用者２が利用する場合に、この利用を制御するシステムである。図１において、このコンテンツ利用制御システム１０は、大きく、著作権者システム２０、コンテンツサーバ３０、ライセンスサーバ４０、および利用者システム５０を有する。

【００５１】著作権者システム２０は、作成したコンテンツを暗号化し、この暗号化した秘匿コンテンツをコンテンツサーバ３０に登録する（Ｓ１０）処理を行う秘匿コンテンツ登録部２１、暗号化したコンテンツ（秘匿コンテンツ）を復号するのに必要なコンテンツ復号キーをライセンスサーバ４０に送出することによって、アクセス制御権をライセンスサーバに委譲する（Ｓ１２）処理を行うアクセス制御権委譲部２２、および利用許可条件（ＡＣＬ）をライセンスサーバ４０に設定する（Ｓ１４）ＡＣＬ設定部２３を有し、著作物のコンテンツに関する利用制御を管理する。

【００５２】コンテンツサーバ３０は、著作権者システム２０から送られた秘匿コンテンツを登録し、利用者システム５０からの秘匿コンテンツ配布要求があった（Ｓ１６）場合に、この登録され、保存されている秘匿コンテンツを暗号化された状態で利用者システム５０に送出する（Ｓ１７）。

【００５３】ライセンスサーバ４０は、ライセンス許可／生成部４１とＬＤＡＰシステム４２とを有する。ライセンス許可／生成部４１は、利用者システム５０からコンテンツの利用要求があった（Ｓ１８）場合、この利用要求に付加された物理要素ＩＤ証明書とこれに対応する復号キーをＬＤＡＰシステム４２から検索し、物理要素ＩＤを復号し、利用要求されたコンテンツに対応するコンテンツ復号キーを検索し、この検索したコンテンツ復号キーを物理要素ＩＤで暗号化したライセンスを送信する（Ｓ２１）。

【００５４】このライセンスは、物理環境特定要素条件であり、物理要素の構造に対応させ、論理和と論理積を用いて構造化した組み合わせの形態となっている。また、この実施の形態では、従来から用いられていた物理環境特定要素条件のみならず、利用者の利用状況を条件とした会計条件も併せてＡＣＬとして暗号化される。このライセンスの暗号化と復号化については後述する。なお、利用要求（Ｓ１８）に物理要素ＩＤ証明書が付加されていない場合、ＬＤＡＰシステム４２内にも存在しない場合には、物理要素条件指定（Ｓ１９）を利用者システム５０に送付して、利用者システム５０が生成した物理要素ＩＤ証明書群を返す（Ｓ２０）。

【００５５】一方、著作権者システム２０からアクセス制御権委譲によるコンテンツ復号キーが送られてきた（Ｓ１２）場合は、このコンテンツ復号キーを後述するＬＤＡＰシステム４２内のキー４４のデータベースに秘匿コンテンツに対応させて登録する。また、著作権者システム２０からＡＣＬ設定が送られてきた（Ｓ１４）には、このＡＣＬを秘匿コンテンツに対応させて、ＬＤＡＰシステム４２内のアクセス制御リスト（ＡＣＬ）に格納する。

【００５６】利用者システム５０は、秘匿コンテンツの配布要求（Ｓ１６）と配布された秘匿コンテンツの取得を行う秘匿コンテンツ要求／取得部５１と、ライセンスの要求、すなわち利用要求（Ｓ１８）とライセンスの取得（Ｓ２１）の処理を行うライセンス要求／取得部５２と、利用者システムの特定利用環境（ＳＵＥ）５３とを有する。特定利用環境５３とは、特定のコンテンツ利用環境をいい、ＣＰＵ、周辺装置、リムーバルな記憶媒体、ＩＣカード、コンテンツ利用状況などの総合的情報をいう。

【００５７】特定利用環境には、ＣＰＵ等の利用環境特定物理要素（ＰＣＳＵＥ）５４－１～５４－Ｎと、コンテンツを格納するコンテンツストレージデバイス５５－１～５５－Ｍと、プレーヤやビューワ等の再生デバイス５６－１～５６－Ｌとを有する。各ＰＣＳＵＥ５４－１～５４－Ｎ，各コンテンツストレージデバイス５５－１～５５－Ｍ，および各再生デバイス５６－１～５６－Ｌは、それぞれの物理要素ＩＤ５７－１～５７－Ｎ，５９－１～５９－Ｍ，６１－１～６１－Ｌを有するととも

に、暗号化／復号化／評価部５８－１～５８－Ｎ，６０－１～６０－Ｍ，６２－１～６２－Ｌを有する。

【００５８】暗号化／復号化／評価部５８－１～５８－Ｎ，６０－１～６０－Ｍ，６２－１～６２－Ｌは、各物理要素を暗号化する場合には、自物理要素の物理要素ＩＤで暗号化して出力し、各物理要素の復号化を行う場合には、自物理要素の物理要素ＩＤで復号化を行い、さらに復号結果を評価する処理を行う。すなわち、各物理要素ＩＤの処理に関しては各物理要素毎に行い、物理要素間のインターフェース上であっても、情報が漏れないようにしている。

【００５９】つぎに上述した著作権者システム２０、コンテンツサーバ３０、ライセンスサーバ４０、利用者システムの動作処理を主としてフローチャートを参照して説明する。まず、図２のフローチャートを参照して、著作権者システム２０の内部処理手順について説明する。

【００６０】図２において、著作権者システム２０は、まず操作イベントが発生したか否かを判断する（ステップＳ１００）。操作イベントが発生していない場合（ステップＳ１００，なし）には、操作イベントが発生するまでこの処理を繰り返し、操作イベントが発生した（ステップＳ１００，あり）には、操作イベントの操作内容が秘匿コンテンツ登録か、ＡＣＬ登録か、アクセス制御権委譲かを判断する（ステップＳ１０１）。

【００６１】操作内容が秘匿コンテンツ登録である場合（ステップ１０１，秘匿コンテンツ登録）には、秘匿コンテンツ登録部２１は、コンテンツの暗号化を行い（ステップＳ１１０）、コンテンツサーバリストから所望のコンテンツサーバ３０を指定し（ステップＳ１１１）、この指定したコンテンツサーバ３０に対して秘匿コンテンツ登録要求を行う（ステップＳ１１２）。その後、コンテンツサーバ３０からの応答を得て、その応答がＯＫであるかエラーであるかを判断する（ステップＳ１１３）。

【００６２】コンテンツサーバ３０からの応答がＯＫの場合にはそのまま、エラーである場合には、エラー処理を行った（ステップＳ１１４）後、さらに、つぎのコンテンツサーバが指定されたか否かを判断する（ステップＳ１１５）。つぎのコンテンツサーバが指定された場合（ステップＳ１１５，あり）には、ステップＳ１１２に移行して上述した処理を繰り返し、つぎのコンテンツサーバが指定されていない場合（ステップＳ１１５，なし）には、ステップＳ１００に移行して上述した処理を繰り返す。

【００６３】操作内容がＡＣＬ設定である場合（ステップ１０１，ＡＣＬ設定）、ＡＣＬ設定部２３は、さらに、指定されたコンテンツ復号キーを登録するか否かを判断し（ステップＳ１２０）、コンテンツ復号キーの登録をしない場合（ステップＳ１２０，なし）には、エラー処理を行って（ステップＳ１２４）、ステップＳ１００に移行し、上述した処理を繰り返す。一方、コンテンツ復号キーの登録がある場合（ステップＳ１２０，あり）には、ＡＣＬ設定要求をライセンスサーバ４０に送信し（ステップＳ１２２）、ライセンスサーバ４０からＡＣＬ登録結果を受信し（ステップＳ１２３）、その後ステップＳ１００に移行して上述した処理を繰り返す。

【００６４】また、操作内容がアクセス制御権委譲である場合（ステップＳ１０１，アクセス制御権委譲）には、暗号化したコンテンツ復号キーをライセンスサーバ４０に送信し（ステップＳ１３０）、暗号化コンテンツ復号キーの登録結果を受信し（ステップＳ１３１）、ステップＳ１００に移行し、上述した処理を繰り返す。

【００６５】つぎに、ここで、ＡＣＬ設定部２３によって設定されるＡＣＬについて説明する。図３は、アクセス条件の一例を示す図であり、アクセス条件は、会計条件と物理環境特定要素（ＰＣＳＵＥ）条件との２種類がある。図３に示すように、本発明の特徴の一つである会計条件としては、まず、maxCount（操作可能回数最大値）があり、これに対応するコンテンツの利用状況はcount（操作済回数）である。操作済回数という可変値に対して操作可能回数最大値という制限を設けてアクセスを制御、すなわち限定と認可を行おうとするものである。

【００６６】つぎのmaxLength（読み出し最大長さ）の会計条件値に対応するコンテンツの利用状況は、totalLen（読み出し済長さ＋被請求読み出し長さ）であり、コンテンツの読み出し最大長さによってアクセスの制御をしようとするものである。つぎのmaxTimeLen（実行可能最大時間）の会計条件値に対応するコンテンツの利用状況は、totalTime（実行済時間長）であり、コンテンツの実行可能最大時間によってアクセスの制御をしようとするものである。つぎのmaxDebt（借入可能金額（課金条件））の会計条件値に対応するコンテンツの利用状況は、debt（残金）であり、残金のマイナス値は借入金額となり、課金条件によってアクセスの制御をしようとするものである。

【００６７】また、物理環境特定要素条件としては、まず計算機本体があり、これに対応する物理要素ＩＤのクラスは、ＰＳＮであり、プロセッサのシリアル番号である。ここで、クラスとはデータベース上のオブジェクトクラスである。つぎの周辺デバイスに対応する物理要素ＩＤのクラスは、ＤＳＮであり、デバイスの種類とシリアル番号を示す。つぎのメディアに対応する物理要素ＩＤのクラスは、ＭＳＮであり、メディアの種類とシリアル番号を示す。つぎのＩＣカードに対応する物理要素ＩＤは、certificatesであり、ＩＣカードが発行する証明書を示す。

【００６８】つぎの人体部位は、たとえば指紋や網膜（アイリス）情報であり、これに対応する物理要素ＩＤのクラスは、bodyPartsであり、人体部位の認証情報で

ある。つぎの許可する時間帯に対応する物理要素ＩＤのクラスは、timePeriodであり、ローカルクロックやグローバルなＧＰＳ時刻である。つぎのネットワークドメインは、ネットワーク上のエリアを示し、これに対応する物理要素ＩＤのクラスは、MACAddressであり、ＭＡＣアドレスを示す。つぎの地理的位置は、利用国などを示し、これに対応する物理要素ＩＤのクラスは、locationであり、ＧＰＳあるいはＰＨＳが検出する位置を示す。つぎの人の記憶に対応する物理要素ＩＤのクラスは、user-ID WithPwdであり、ユーザＩＤとパスワードを示す。最後のグループに対応する物理要素ＩＤのクラスは、groupであり、物理要素ＩＤの集合を示す。

【００６９】このようなアクセス条件は、ＡＮＤとＯＲとの論理的な組み合わせをもったセット、すなわちＡＣＬとして設定される。アクセス条件には、上述したように会計条件と物理環境特定要素条件とがあるが、これらは任意に組み合わせ可能である。たとえば、一つのＡＣＬとしては、つぎのようなものが設定される。すなわち、

udac#acl
read:((grop=sysrapＯＲ group=soft4soft) ＡＮＤ 45661244<ＭＳＮ<45661412) ＯＲ count<1;
modify:user=yujiＯＲ user=hataＯＲ IC#card=1afd234fe4def458c3bac78497bbda6f;
print:group=sysrap;

のようなＡＣＬを設定することができる。

【００７０】この設定されたＡＣＬによれば、「read」は閲覧条件を示し、グループが「sysrap」あるいは「soft4soft」であり、かつ、メディアシリアル番号ＭＳＮが45661244を越え45661412未満であるか、あるいは操作済回数が１未満すなわち、一度もコンテンツを利用したことがないことが閲覧のための条件となる。さらに、「modify」は更新条件を示し、ユーザ名が「yuji」あるいは「hata」であるか、あるいは「IC#card」の番号が「1afd234fe4def458c3bac78497bbda6f」であることがコンテンツ更新のための条件となる。

【００７１】また、「print」は印刷出力条件を示し、グループが「sysrap」に限り、コンテンツを印刷することができる。このようなＡＣＬは、著作権者システム２０から著作権者１が任意に設定することができる。このＡＣＬ設定は、ＧＵＩを用いることによって操作性が向上する。なお、ＡＣＬのタイプは、操作名とともに設定するようにしてもよい。たとえば、操作名１に対してはアクセス条件（１）なる条件を選択でき、操作名２に対してはアクセス条件（２）なる条件を選択できるようにしてもよい。これにより、さらに操作性が向上する。

【００７２】つぎに、図４に示すフローチャートを参照して、コンテンツサーバ３０の内部処理手順について説明する。図４において、まずコンテンツサーバ３０は、ネットワークイベントが入力されたか、入力された場合に秘匿コンテンツ登録要求か、秘匿コンテンツ配布要求かを判断する（ステップＳ２００）。ネットワークイベントが入力されない場合（ステップＳ２００，なし）には、ステップ２００における判断処理を繰り返す。

【００７３】ネットワークイベントが秘匿コンテンツ登録要求である場合（ステップＳ２００，秘匿コンテンツ登録要求）には、この登録要求された秘匿コンテンツを内部登録し（ステップＳ２１０）、デフォルトのＡＣＬを設定する（ステップＳ２１１）。そして、著作権者システム２０に、この秘匿コンテンツ登録要求に対する応答を行って（ステップＳ２１２）、ステップＳ２００に移行し、上述した処理を繰り返す。

【００７４】一方、ネットワークイベントが秘匿コンテンツ配布要求である場合（ステップＳ２００，秘匿コンテンツ配布要求）には、この配布要求された秘匿コンテンツを利用者システム５０に対して配布し（ステップＳ２２０）、その後、この秘匿コンテンツ配布要求に対する応答を利用者システム５０に対して行い（ステップＳ２２１）、ステップＳ２００に移行して上述した処理を繰り返す。これにより、コンテンツサーバ３０を介して秘匿コンテンツを秘密状態で著作権者システム２０から利用者システム５０に配布することができる。この場合、トラフィックが分散され、高速転送が可能であるとともに、予め利用者システム５０の近傍のコンテンツサーバまで秘匿コンテンツを保持することが可能であるので、配布処理を高速に処理することができる。

【００７５】つぎに、図５に示すフローチャートを参照して、ライセンスサーバ４０の内部処理手順について説明する。図５において、まず、ライセンスサーバ４０は、コンテンツ利用要求のネットワークイベントが入力されたか否かを判断する（ステップＳ３００）。ネットワークイベントが入力されない場合（ステップＳ３００，なし）には、このステップＳ３００の判断処理を繰り返す。

【００７６】ネットワークイベントがコンテンツ利用要求である場合（ステップＳ３００，コンテンツ利用要求）には、指定されたコンテンツのＡＣＬをＬＤＡＰシステム４２から検索し（ステップＳ３０１）、さらに、この検索したＡＣＬから関連するアクセス条件を抽出し、新たなＡＣＬを生成する（ステップ３０２）。その後抽出した物理環境特定条件に対応する対応物理要素ＩＤ証明書があるか否かを判断し（ステップＳ３０３）、対応物理要素ＩＤ証明書がある場合（ステップＳ３０３，対応物理要素ＩＤ証明書あり）にはそのまま、対応物理要素ＩＤ証明書が無い場合（ステップＳ３０３，対応物理要素ＩＤ証明書無し）には、コンテンツの利用要求者に対して、すなわち利用者システム５０に対して証明書を要求した（ステップＳ３０４）後、さらに、つぎの物理環境特定条件があるか否かを判断する（ステップＳ３０５）。

【００７７】つぎの物理環境特定条件がある場合（ステップＳ３０５，あり）には、ステップＳ３０３に移行して対応物理要素ＩＤ証明書を確実に備える準備をし、つぎの物理環境特定条件がない場合（ステップＳ３０５，なし）には、コンテンツの利用要求者、すなわち利用者システム５０から物理要素ＩＤ証明書群を受信する（ステップＳ３０６）。

【００７８】その後、ライセンス許可／生成部４１は、指定されたコンテンツ復号キーを検索し（ステップＳ３０７）、ＡＣＬ内のアクセス条件を、強制可能な物理要素の証明書に並べ直す（ステップＳ３０８）。さらに、ＡＣＬ内のすべてのＡＮＤ／ＯＲ式を認証優先順に括弧でくくる処理を行う（ステップＳ３０９）。その後ライセンス許可／生成部４１は、この括弧でくくられたＡＮＤ／ＯＲ式をもとに、ライセンスを生成するライセンス生成処理を行う（ステップＳ３１０）。そして、生成されたライセンスを利用者システム５０に送信し（ステップＳ３１１）、ステップＳ３００に移行して上述した処理を繰り返す。

【００７９】ここで、生成されたライセンスと秘匿コンテンツとの関係について図６を参照して説明する。図６は、ライセンスサーバ４０から利用者システム５０に送信されるライセンスとコンテンツサーバ３０を介して著作権者システム２０から利用者システム５０に送信される秘匿コンテンツとの関係を示している。

【００８０】図６において、ライセンスサーバ４０のＡＣＬ４３内には、それぞれ各秘匿コンテンツ７１～７５と対応づけられたシステムＡＣＬ４３－１～４３－５が格納されている。このシステムＡＣＬをもとにその後、たとえば秘匿コンテンツ７１～７３に対応するシステムＡＣＬから秘匿コンテンツ７１～７３に対するライセンス８４～８６が生成され、利用者システムに送信される。このライセンス８４～８６は、対応する物理要素ＩＤで暗号化されており、外部に情報が漏れることはない。利用者システム５０は、ライセンス８４～８６からクライアントＡＣＬ８１～８３を復号し、これらに対応する秘匿コンテンツ７１’～７３’を復号し、それぞれコンテンツを得ることができる。

【００８１】この場合、秘匿コンテンツも暗号化されているので、セキュリティは十分である。このようにして、ＡＣＬと秘匿コンテンツとはその秘匿状態を維持しながら、それぞれ転送ルートが異なるものの、対応づけられている。なお、コンテンツサーバ３０を含む転送経路を介して送られる秘匿コンテンツの状態は、仮想格納領域７０として表現している。

【００８２】ここで、さらにライセンスサーバ４０内のＬＤＡＰシステム４２について図７を参照して説明する。図７において、ＬＤＡＰシステム４２は、複数のＬＤＡＰサーバを有し、そのクライアントサーバとしてライセンスサーバ４０が位置づけられ、ライセンスサーバ４０の管理のもとに各ＬＤＡＰサーバが機能することになる。ＬＤＡＰサーバとは、ディレクトリサービスの標準であるＸ．５００に含まれるＤＡＰの軽量版のプロトコルを用いたディレクトリサーバである。ＬＤＡＰサーバ内には複数のクラスに分けられ、たとえば個人情報９１、システムクラス９２、メディアクラス９３、ＸＭＬで記述されたＸＭＬ情報のクラスを有する。

【００８３】そして、たとえば個人情報９１のクラスにおいて、「own system」が検索されると、このシステムをシステムクラス９２から「system name」によって検索し、さらにシステムクラス９２内の現メディア「current media」は、メディアクラスの中からメディアクラス９３を検索し、さらに、このメディアクラス９３内のコンテンツから、このコンテンツに対応したＸＭＬ情報９４を検索することができる。このＸＭＬ情報９４の中には、コンテンツに関する情報が格納されている。

【００８４】ところで、利用者システム５０の特定利用環境は、図８に示すレイヤを持った論理構造を有している。図８では、特定利用環境１００が、アプリケーション層１１０とＯＳカーネル層１１１とデバイス層１１２との３層で構成され、各層間は、点線で示すサービスインターフェースで接続される。アプリケーション層１１０は、コンテンツ再生・実行アプリケーション１０１を有し、内部には、秘密コンテンツ復号保護ライブラリ１０２をプログラムモジュールとして有する。

【００８５】秘密コンテンツ復号保護ライブラリ１０２は、ストレージドライバ１０３、ファイルシステム１０５、複数の利用環境特定物理要素ドライバ１０６～１０８、再生デバイスドライバを動作させる。ストレージドライバ１０３は、コンテンツストレージデバイスを駆動させ、利用環境特定物理要素ドライバ１０６～１０８はそれぞれ利用環境特定物理要素１０９～１１１を駆動させ、再生デバイスドライバ１１２は再生デバイス１１３を駆動させる。なお、一つの物理装置であっても、たとえばＭＯ装置のようにコンテンツストレージデバイス１０４と利用環境特定要素１０９の二つの役割を担ってもよい。

【００８６】図９は、利用環境特定物理要素（ＰＣＳＵＥ）のＯＳカーネル層１１１とデバイス層１１２との対応関係を示している。図９に示すように、ＰＣＳＵＥ同士は、包含関係を持つことがある。もちろん、デバイス層１１２における他のデバイスも同様である。たとえば、ＰＣＳＵＥ１３１の下位にはＰＣＳＵＥ１３３，１３４が位置づけられ、ＰＣＳＵＥ１３４の下位にはＰＣＳＵＥ１３５，１３６が位置づけられる。このような包含関係を有するＰＣＳＵＥ同士では、物理要素ＩＤ等の情報をデータ交換することができる。

【００８７】たとえば、ＤＶＤ装置等のメディア再生装置のＰＣＳＵＥは、ＤＶＤ等のメディアのＰＣＳＵＥを包含しており、コンテンツデータやメディアＩＤ情報を

両者間で交換する。たとえば、ＰＣＳＵＥ１３４とＰＣＳＵＥ１３５との間の情報交換である。そして、最上位のＰＣＳＵＥのみがＰＣＳＵＥドライバとのデータ交換を行う。たとえば、ＰＣＳＵＥドライバ１２０とＰＣＳＵＥ１３１との関係である。従って、同じデバイス層であっても、包含関係を有し、階層的な関係を有する場合がある。

【００８８】ライセンスは、上述したように、特定環境に対する許諾情報であり、ライセンスを要求したクライアント環境、すなわち利用者システムの環境に固有の情報のみを含むものであり、ＡＣＬとコンテント復号キーＫｃとからなるアクセス情報を物理要素ＩＤ（ＰＣＳＵＥ－ＩＤ）によって暗号化されたものである。

【００８９】ここで、多重化されたライセンスの一例を示すと、つぎのようになる。すなわち、

【数１】

$$\{\{\{\{<\text{アクセス情報}>\}K_6\}K_4\}K_3\}K_2\}K_1$$

である。ここで、K_1～K_6は、それぞれＰＣＳＵＥ－ＩＤである。このライセンスは、アクセス情報はK_1～K_6を用いてＡＮＤ条件によって結合されている。物理要素のセキュリティ強度が高い順に各ＰＣＳＵＥ－ＩＤを用いて多重的に暗号化するとよい。この復号化は、この逆に外側のＰＣＳＵＥ－ＩＤから順次復号されることになる。

【００９０】また、物理要素のセキュリティ強度がほぼ同一の場合には、各ＰＣＳＵＥ－ＩＤを排他的論理和演算によってその結果の暗号キーによって復号できるようにしてもよい。たとえば、

【数２】

$$\{<\text{アクセス情報}>\}(K_6 \oplus K_4 \oplus K_3 \oplus K_2 \oplus K_1)$$

のようにするとよい。これらの暗号化の多重化によって、一部の製品、すなわち一部の物理要素への攻撃成功によるコンテンツ復号キーＫｃ盗難の危険性が分散されるという、リスク分散の効果をもたらすことになる。

【００９１】また、複数のＰＣＳＵＥ－ＩＤをＯＲ演算子で結合する場合、すなわち、

【数３】

$$\{<\text{アクセス情報}>\}K_6 + \{<\text{アクセス情報}>\}K_5 + \{<\text{アクセス情報}>\}K_3 + \{<\text{アクセス情報}>\}K_2 + \{<\text{アクセス情報}>\}K_1$$

のような場合には、それぞれのＰＣＳＵＥ－ＩＤで暗号化されたサブライセンス、たとえば、$\{<\text{アクセス情報}>\}K_1$を生成し、すべてのサブライセンスを単純にＯＲ演算して結合した値をライセンスとしてもよい。この場合、上述した暗号化の多重化を各サブライセンスにも適用し、ＡＮＤ、ＸＯＲ、ＯＲ演算を入れ子にして組み合わせたライセンスとして生成してもよい。これによっても、リスク分散の効果は得られる。

【００９２】つぎに、このようなライセンスの生成処理手順について図１０に示すフローチャートを参照して説明する。この図１０に示すフローチャートは、図５のステップＳ３１０に示すライセンス生成処理手順のサブルーチンである。図５において、まず、上述したＡＣＬから１ワード読み出す（ステップＳ４００）。その後読み出したワードが「（」であるか否かを判断する（ステップＳ４１０）。

【００９３】読み出したワードが「（」である場合（ステップＳ４１０，「（」）には、ＡＣＬの読み出し現在位置を括弧内ＡＣＬの始点として記憶する（ステップＳ４１１）。その後、変数ＮＢを「０」に設定し（ステップＳ４１２）、さらにＡＣＬから１ワード読み出す（ステップＳ４１３）。その後、読み出したワードが「（」であるか否かを判断し（ステップＳ４１４）、「（」である場合には、変数ＮＢに「１」を加算した（ステップＳ４１５）後、ステップＳ４１３に移行して再び、つぎの１ワードを読み出す。

【００９４】一方、読み出しワードが「（」でない場合（ステップＳ４１４，その他）には、さらにこの読み出したワードが「）」であるか否かを判断する（ステップＳ４１６）。この読み出したワードが「）」でない場合、すなわちその他である場合には、ステップＳ４１３に移行し、さらにＡＣＬから１ワードを読み出す。一方、この読み出したワードが「）」である場合には、ＮＢが「０」であるか否かを判断する（ステップＳ４１７）。ＮＢが「０」でない場合（ステップＳ４１７，ＮＯ）には、ＮＢの値から「１」減算し、ステップＳ４１３に移行し、さらにＡＣＬから１ワード読み出す。

【００９５】ＮＢが「０」のとき（ステップＳ４１７，ＹＥＳ）には、ＡＣＬの現在位置の一つ手前を括弧内ＡＣＬの終点として記憶する（ステップＳ４１９）。その後、この括弧内ＡＣＬのライセンス生成処理を行い（ステップＳ４２０）、その再帰呼び出しによる戻り値をアクセス条件ＡＣに追加する処理を行って（ステップＳ４２１）、ステップＳ４００に移行する。これによって括弧内のＡＣＬが生成される。

【００９６】一方、読み出したワードが「（」でない場合（ステップＳ４１０，その他）には、さらに、この読み出したワードが物理要素条件または会計条件であるか否かを判断する（ステップＳ４１０）。物理条件または会計条件である場合には、この条件をアクセス条件ＡＣに設定し（ステップＳ４３１）、この条件を強制可能な物理要素の秘密キーＫｐとして設定し（ステップＳ４３２）、ステップＳ４００に移行し、さらにＡＣＬから１ワード読み出す。

【００９７】読み出したワードが物理条件または会計条件でない場合（ステップＳ４１０，その他）には、さらに、この読み出したワードが「ＯＲ」であるか否かを判

断する（ステップＳ４３０）。読み出したワードが「ＯＲ」である場合には、この読み出したワードから後のＡＣＬのライセンス生成処理を行う（ステップＳ４４１）。その後、さらに生成したライセンスの中にＡＣが含まれるか否かを判断し（ステップＳ４４２）、ＡＣが含まれる場合（ステップＳ４４２，ＹＥＳ）には、ステップＳ４４１によるライセンス生成処理の戻り値を用いて「{ＡＣ，hash} Ｋｐ，戻り値」となるライセンスに設定し（ステップＳ４４３）、この生成したライセンスを返す（ステップＳ４５４）。一方、ライセンスの中にＡＣが含まれていない場合（ステップＳ４４２，ＮＯ）には、ステップＳ４４１によるライセンス生成処理の戻り値を用いて「{Ｋｃ，ＡＣ，hash} Ｋｐ，戻り値」となるライセンスに設定し（ステップＳ４４５）、この生成したライセンスを返す（ステップＳ４５４）。

【００９８】一方、読み出したワードが「ＯＲ」でない場合（ステップＳ４３０，その他）には、さらに、この読み出したワードが「ＡＮＤ」であるか否かを判断する（ステップＳ４４０）。読み出したワードが「ＡＮＤ」である場合には、この読み出したワードから後のＡＣＬのライセンス生成処理を行い（ステップＳ４５２）、このライセンス生成処理の戻り値を用いて「{戻り値，ＡＣ，hash} Ｋｐ」となるライセンスを返す（ステップＳ４５４）。

【００９９】さらに、この読み出したワードが「ＡＮＤ」でない場合（ステップＳ４４０，その他）には、「{Ｋｃ，ＡＣ，hash} Ｋｐ」となるライセンスを返す（ステップＳ４５４）。これにより、ＡＣＬからライセンスが生成される。

【０１００】つぎに、図１１に示すフローチャートを参照して、利用者システム５０の内部処理手順について説明する。図１１において、まず利用者システム５０は、コンテンツの利用要求があったか否かを判断する（ステップＳ５００）。コンテンツの利用要求がない場合（ステップＳ５００，なし）には、この判断処理を繰り返し、コンテンツの利用要求があった場合（ステップＳ５００，あり）には、コンテンツの利用要求を送信する（ステップＳ５０１）。その後、物理要素の証明書の要求がライセンスサーバ４０からあったか否かを判断し（ステップＳ５０２）、物理要素の証明書の要求がない場合（ステップＳ５０２，なし）には、ステップＳ５０８に移行する。

【０１０１】一方、物理要素の証明書の要求があった場合（ステップＳ５０２，あり）には、物理要素ＩＤ証明書を読み出し（ステップＳ５０３）、読み出し失敗したか否かを判断する（ステップＳ５０４）。読み出しに失敗した場合（ステップＳ５０４，ＹＥＳ）には、エラー通知をライセンスサーバに送信して（ステップＳ５０５）、ステップＳ５００に移行する。一方、読み出しに失敗しない場合（ステップＳ５０４，ＮＯ）には、つぎの物理要素があるか否かを判断し（ステップＳ５０６）、つぎの物理要素がある場合（ステップＳ５０６，あり）には、ステップＳ５０３に移行して、つぎの物理要素ＩＤ証明書の読み出しを行って上述した処理を繰り返す。

【０１０２】一方、つぎの物理要素がない場合（ステップＳ５０６，なし）には、物理要素ＩＤ証明書群をライセンスサーバ４０に送信し（ステップＳ５０７）、さらに受信内容がエラーかライセンスかを判断する（ステップＳ５０８）。受信内容がエラーである場合（ステップＳ５０８，エラー）には、ステップＳ５００に移行して上述した処理を繰り返し、受信内容がライセンスである場合（ステップＳ５０８，ライセンス）には、さらに、ライセンスを物理要素（ＰＣＳＵＥ）１に渡し（ステップＳ５０９）、ステップＳ５００に移行して上述した処理を繰り返す。これにより、利用者システム５０は、ライセンスサーバ４０からライセンスを取得することができる。

【０１０３】ここで、ＰＣＳＵＥ１とは、（Ｎ－１）個のＰＣＳＵＥの最初のＰＣＳＵＥを示し、一般的にＰＣＳＵＥｉで示し、ｉは、１～（Ｎ－１）の整数である。そこで、各ＰＣＳＵＥｉがライセンスを渡された時の内部処理手順について図１２のフローチャートを参照して説明する。

【０１０４】図１２において、まずＰＣＳＵＥｉは、受信したライセンスをKpiで復号する（ステップ６００）。その後、この復号したアクセス条件ＡＣｉを評価し（ステップＳ６０１）、アクセス条件ＡＣｉの評価結果が可か不可かを判断する（ステップＳ６０２）。アクセス条件ＡＣｉの評価結果が不可の場合（ステップＳ６０２，不可）には、エラー処理を行って（ステップＳ６０４）、本処理を終了する。一方、アクセス条件ＡＣｉの評価結果が可である場合（ステップＳ６０２，可）には、この復号したライセンスをＰＣＳＵＥ（ｉ＋１）に送信し、復号を続行させ、本ＰＣＳＵＥｉの内部処理を終了する。

【０１０５】つぎに、ＰＣＳＵＥ（ｉ＋１）は、ＰＣＳＵＥ（Ｎ）に相当し、ここでは、たとえば、再生デバイスの物理要素が内部処理を行う。この内部処理手順について図１３に示すフローチャートを参照して説明する。図１３において、まず、受信したライセンスをKpnで復号する（ステップＳ７００）。その後、この復号したアクセス条件ＡＣ（Ｎ）を評価し（ステップＳ７０１）、この評価結果が可であるか、不可であるかを判断する（ステップＳ７０２）。評価結果が不可である場合（ステップＳ７０２，不可）には、エラー処理を行って（ステップＳ７０３）、本処理を終了して、結果的に秘匿コンテンツを復号することができないことになる。

【０１０６】一方、アクセス条件ＡＣ（Ｎ）に対する評価結果が可である場合（ステップＳ７０２，可）には、

この復号したＫｃで秘匿コンテンツを復号し（ステップＳ７０４）、復号したコンテンツを再生デバイスが再生し（ステップＳ７０５）、本処理を終了する。

【０１０７】ここで、具体的なライセンスの復号処理を図１４を参照して説明する。図１４において、ライセンスサーバ４０で生成されたライセンスは、アクセス制御リストＡＣＬとコンテンツ復号キーとを再生デバイス１４４の物理要素ＩＤであるキーＫｐを用いて暗号化し、さらに、ストレージデバイスのデバイスシリアル番号であるＤＳＮ１４１とメディア１４２のメディアシリアル番号であるＭＳＮ１４３の排他的論理和の値をキーとして暗号化されたものである。

【０１０８】まず、ストレージデバイス１４０は、メディア１４２に書き込み不可のＭＳＮを読み込み、この値とストレージデバイス１４０自身のＤＳＮとの排他的論理和の演算を行い、この演算結果によってライセンスを復号すると、ライセンスは、｛ＡＣＬ，Ｋｃ｝Ｋｐとなる。この一部復号されたライセンスは、再生デバイス１４４に送られ、再生デバイス１４４は、再生デバイス１４４自身が有する物理要素ＩＤであるキーＫｐを用いてライセンスを復号し、アクセス条件リストＡＣＬとコンテンツ復号キーＫｃとを取得し、アクセス条件ＡＣＬが示すアクセス条件を満足する場合に、コンテンツ復号キーＫｃによって復号を行うことができ、復号されたコンテンツは、再生デバイス１４４によって再生されることになる。

【０１０９】上述したライセンス要求とライセンス取得によるコンテンツ復号処理を図１５に示すデータフローを参照してさらに説明する。図１５において、利用者システム５０内における復号保護領域では、まずコンテンツを利用するためライセンス要求処理１５２を物理要素ＩＤ証明書を付してライセンスサーバ４０に送出する。この際、物理要素ＩＤ証明書は、利用環境特定物理要素証明書取得処理１５３によって利用環境特定物理要素１５０から取得され、ライセンス要求処理１５２によって渡される。

【０１１０】一方、ライセンスサーバ４０からライセンスが送信されるとライセンス取得処理１５６は、このライセンスを取得し、アクセス許可処理１５５は、ライセンス所得処理１５６からライセンスを取得するとともに、利用環境特定物理要素ＩＤ認証処理１５４が利用環境特定物理要素証明書取得処理１５３を介して物理要素ＩＤを取得し、さらに会計処理１５７から利用状況を取得し、これらを用いて復号キーを取り出す。

【０１１１】そして、コンテンツ復号処理１５９は、コンテンツ復号キーを用いて秘匿コンテンツ１５８を復号し、平文のコンテンツを出力する。なお、会計処理１５７は、利用状況監視物理要素１５１に通知し、利用環境監視物理要素１５１によって現在の利用状況が利用に応じて自動的にデクリメントされる。

【０１１２】ところで、図１６は、図８に示した特定利用環境の各エンティティに各処理手続きを実装した場合の保護強度への影響を示す図である。この結果から、利用環境特定物理要素所有証明書の生成は、デバイス層に実装し、会計情報保護は、ＩＣカードによるデバイス層に実装することが好ましいことがわかる。このように、各処理手続きを実装するレイヤによっても保護強度が異なるので、レイヤ配置も考慮して図１５に示す各処理機能を実装する必要がある。

【０１１３】なお、上述した実施の形態では、いわゆるコンテンツキャッシュ可能型モデルを基準とした構成として説明したが、これに限らず、コンテンツ同時配布型モデルを基準とした構成にも適用できるのは明らかである。この場合、コンテンツサーバ３０がライセンスサーバ４０内に内部配置された構成として取り扱えばよい。

【０１１４】さらに、上述した実施の形態では、暗号化、復号化に関して、キーを用いることが前提となっているが、この場合において、秘密鍵暗号方式を用いても、公開鍵暗号方式を用いても、いずれでも実施可能であり、適応されるシステムに応じてそれぞれ適切な方式を適用すればよい。

【０１１５】また、上述した実施の形態に示す物理要素には、利用者システム５０に固定の装置のみではなく、この利用者システム５０を利用する際に用いられるメディア、すなわちＣＤ－ＲＯＭ、ＤＶＤ、ＭＯ、ＩＣカードやフロッピーディスク等の可搬型の記録媒体を含むものである。この可搬型の記録媒体が用いられる利用者システムにおいては、この利用者システムに固定の物理要素に加えて、この用いられる可搬型の記録媒体も物理要素に含まれて、コンテンツの利用制御がなされることになる。なお、利用者システム５０に固定のメディア、例えば固定のハードディスク装置や固定のＲＯＭ等が上述した物理要素に含まれるのは言うまでもない。

【０１１６】

【発明の効果】以上説明したように、請求項１にかかる発明によれば、設定手段が、前記利用者手段内で使用するメディアを含む当該利用者手段の物理要素に関する識別情報および前記利用者に関する識別情報に基づいた前記コンテンツに対する複数の部分利用許可条件をさらに論理和および論理積の組み合わせによって構造化表現した利用許可条件として設定し、前記利用制御手段は、前記設定手段によって設定された利用許可条件をもとに前記利用者手段による前記コンテンツの利用を制御し、利用許可条件に基づいた柔軟な利用制御を可能とするようにしているので、この利用許可条件に基づいた柔軟なコンテンツ利用制御を行うことができるという効果を奏する。

【０１１７】また、請求項２にかかる発明によれば、設定手段よって設定される部分利用許可条件は、前記利用者手段および前記利用者の利用状況に応じて変化するカ

テゴリーに対する条件である会計条件を含むようにしているので、一層利用者に対するコンテンツ利用制御を細かにかつ柔軟に行うことができるという効果を奏する。

【０１１８】また、請求項３にかかる発明によれば、生成手段が、前記利用者手段からのコンテンツ利用要求を受けて、前記利用許可条件および前記コンテンツの復号キーを前記利用者手段内で使用するメディアを含む当該利用者手段の複数の物理要素に関する識別情報によって暗号化した許諾情報を生成し、前記利用者手段は、前記コンテンツ利用要求に応じて送られる前記許諾情報を当該利用者手段による物理要素の識別情報をもとに復号し、前記利用許可条件を満足する場合に前記コンテンツの復号キーを用いて前記暗号化されたコンテンツの復号を行うようにしているので、保護強度の高いコンテンツ利用制御を行うことができるという効果を奏する。

【０１１９】また、請求項４にかかる発明によれば、利用許可条件内の部分利用許可条件間が論理積で記述されている場合には、当該部分利用許可条件に対応する物理要素の識別情報による暗号化を多重化して行っているので、一部の物理要素に対する攻撃成功によるコンテンツ復号キーの盗難の危険性を分散することができるという効果を奏する。

【０１２０】また、請求項５にかかる発明によれば、物理要素が包含関係にある物理要素であっても一つの物理要素として取り扱ってるので、この一つの物理要素の不正も許さず、コンテンツ復号キーの盗難という危険性を分散することができるという効果を奏する。

【０１２１】また、請求項６にかかる発明によれば、開放ネットワーク上に、前記情報提供権限者手段によって暗号化したコンテンツを保持し、前記利用者手段からのコンテンツ配布要求を受け付けて前記暗号化したコンテンツを当該利用者手段に送付するコンテンツサーバを有しているので、開放ネットワークを十分に活用して当該システムにおけるトラフィックの輻輳を防止して、迅速にコンテンツを獲得することができるという効果を奏する。

【０１２２】また、請求項７にかかる発明によれば、設定手段が、利用者手段内で使用するメディアを含む当該利用者手段の物理要素に関する識別情報および前記利用者に関する識別情報に基づいた前記コンテンツに対する複数の部分利用許可条件をさらに論理和および論理積の組み合わせによって構造化表現した利用許可条件を前記利用制御手段内の条件格納手段に格納することによって予め設定するとともに、保持手段に前記コンテンツの復号キーを保持する。抽出手段は、前記利用者手段からのコンテンツの利用要求を受け付けて当該利用者手段に対応する利用許可条件および前記コンテンツの復号キーを抽出し、前記利用者手段から送付された物理要素の識別情報をもとに前記利用許可条件および前記コンテンツの復号キーを暗号化した許諾情報を生成して当該利用者手段に送出する。利用者手段は、前記コンテンツ利用要求に応じて送られる前記許諾情報を当該利用者手段による物理要素の識別情報をもとに復号し、前記利用許可条件を満足する場合に前記コンテンツの復号キーを用いて前記暗号化されたコンテンツの復号を行うようにしているので、柔軟なコンテンツ利用制御に伴う暗号化、復号化を具体的に実現することができるという効果を奏する。

【０１２３】また、請求項８、９にかかる発明によれば、要求手段が、コンテンツの利用要求に応じて、コンテンツの管理を行うコンテンツ管理装置に、当該コンテンツ利用装置の物理要素に関する識別情報および利用者に関する識別情報を送信すると、その後、前記コンテンツの利用要求に対応してコンテンツ管理装置によって送信される許諾情報から、当該コンテンツ利用装置の物理要素に関する識別情報をもとに復号して利用許可条件およびコンテンツの復号キーを求め、前記求めた利用許可条件を判定し許可される場合に前記求めた復号キーを用いてコンテンツの復号を行うようにしているので、保護強度の高いコンテンツ利用制御を行うことができるという効果を奏する。

【０１２４】また、請求項１０、１１にかかる発明によれば、まず、コンテンツの利用要求に対応して、コンテンツの許諾情報から、当該コンテンツ利用装置の物理要素に関する識別情報をもとに復号して利用許可条件およびコンテンツの復号キーを求め、その後、前記求めた利用許可条件を判定し許可される場合に、前記求めた復号キーを用いてコンテンツの復号を行うようにしているので、一層保護強度の高いコンテンツ利用制御を行うことができるという効果を奏する。

【図面の簡単な説明】

【図１】本発明の一実施の形態であるコンテンツ利用制御システムの構成を示す図である。

【図２】図１に示した著作権者システム２０の内部処理手順を示すフローチャートである。

【図３】会計条件と物理環境特定要素条件との一例を示す図である。

【図４】図１に示したコンテンツサーバ３０の内部処理手順を示すフローチャートである。

【図５】図１に示したライセンスサーバ４０の内部処理手順を示すフローチャートである。

【図６】ライセンスサーバ４０から送られるライセンスと著作権者システム１０あるいはコンテンツサーバ３０から送られる秘匿コンテンツとの関係を示す図である。

【図７】図１に示したＬＤＡＰシステム４２の構成を示す図である。

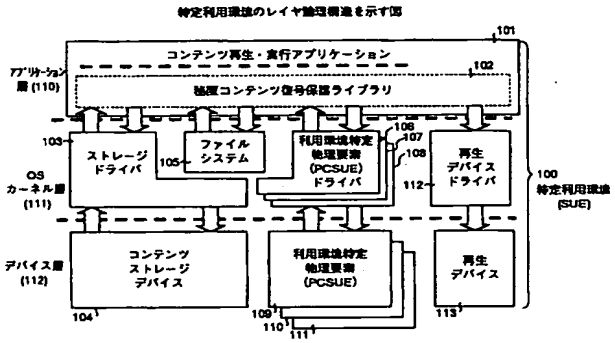
【図８】特定利用環境のレイヤ論理構造を示す図である。

【図９】包含関係をもった物理要素の一例を示す図である。

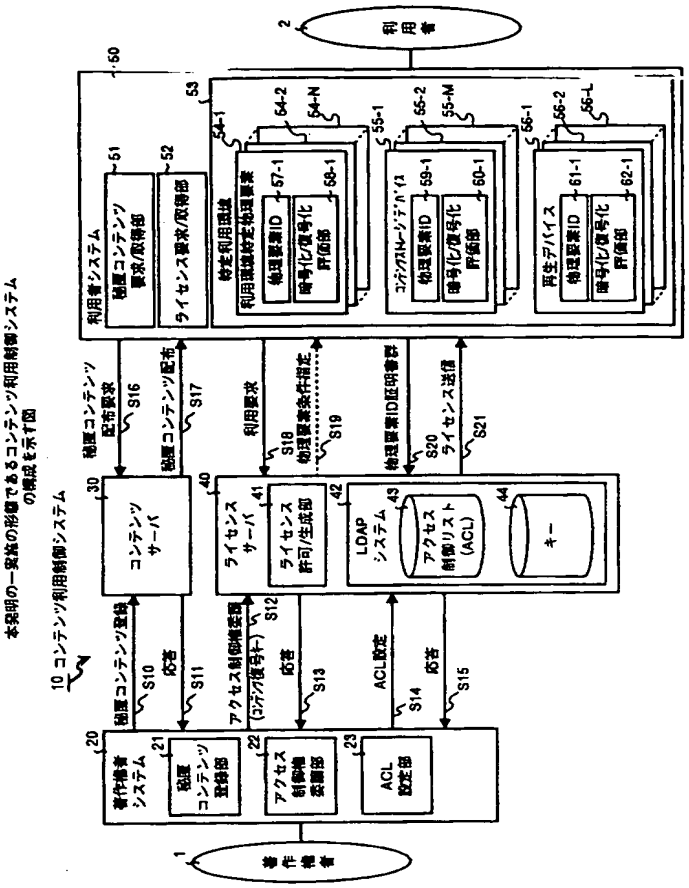
【図１０】ライセンス生成処理手順を示す詳細フローチ

ャートである。
【図１１】図１に示した利用者システム５０の内部処理手順を示すフローチャートである。
【図１２】利用関係特定物理要素によるライセンス復号処理手順を示すフローチャートである。
【図１３】再生デバイスの物理要素によるライセンス復号処理手順を示すフローチャートである。
【図１４】ライセンスの復号過程の一例を示す図である。
【図１５】ライセンス要求とライセンス取得によるコンテンツ復号処理を示すデータフロー図である。
【図１６】特定利用環境の各エンティティに各処理手続きを実装した場合における保護強度への影響を示す図である。
【図１７】従来におけるアクセス制御モデルを示す図である。
【図１８】従来におけるアクセス制御モデルに対応したコンテンツ利用制御システムの概要構成を示す図である。
【図１９】改良したアクセス制御モデルを示す図である。
【図２０】従来におけるコンテンツ利用制御システムのコンテンツ配布モデルを示す図である。
【図２１】コンテンツキャッシュ可能型モデルを示す図である。
【図２２】図２１に示したコンテンツキャッシュ可能型モデルに対応するコンテンツ利用制御システムの概要構成を示す図である。
【図２３】コンテンツ同時配布型モデルを実現するコンテンツ利用制御システムの概要構成を示す図である。
【符号の説明】
１　著作権者
２　利用者
１０　コンテンツ利用制御システム
２０　著作権者システム
２１　秘密コンテンツ登録部
２２　アクセス制御権委譲部
２３　ＡＣＬ設定部
３０　コンテンツサーバ
４０　ライセンスサーバ
４１　ライセンス許可／生成部
４２　ＬＤＡＰシステム
４３　アクセス制御リスト（ＡＣＬ）
４４　キー
５０　利用者システム
５１　秘匿コンテンツ要求／取得部
５２　ライセンス要求／取得部
５３　特定利用環境
５４－１～５４－Ｎ　利用環境特定物理要素
５５－１～５５－Ｍ　コンテンツストレージデバイス
５６－１～５６－Ｌ　再生デバイス
５７－１、５９－１、６１－１　物理要素ＩＤ
５８－１、６０－１、６２－１　暗号化／復号化／評価部

【図８】

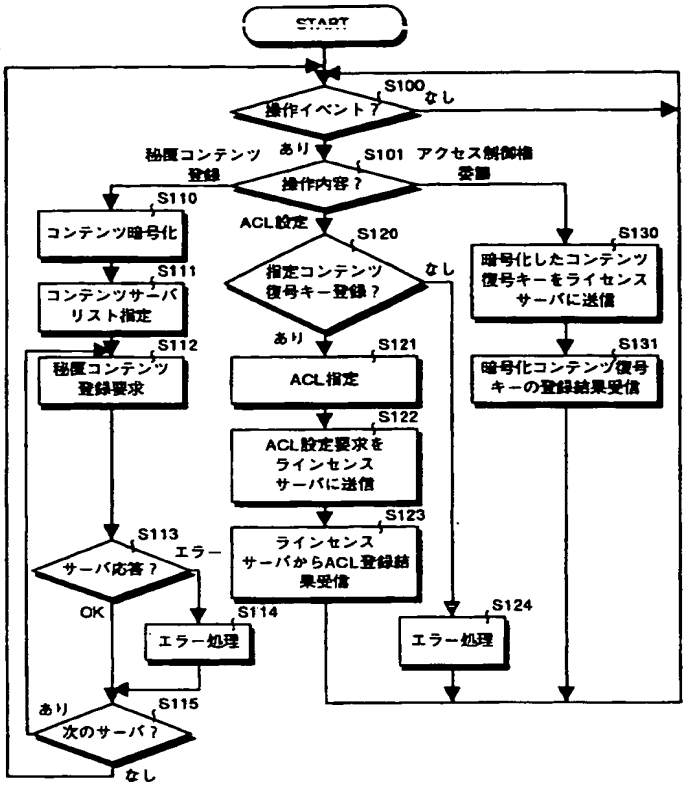


【図１】


本発明の一実施の形態であるコンテンツ利用制御システムの構成を示す図
10 コンテンツ利用制御システム
1 著作権者
2 利用者
20 著作権者システム
21 秘匿コンテンツ登録部
22 アクセス制御情報登録部
23 ACL設定部
30 コンテンツサーバ
40 ライセンスサーバ
41 ライセンス許可/生成部
42 LDAPシステム
43 アクセス制御リスト(ACL)
44 キー
50 利用者システム
51 秘匿コンテンツ要求/取得部
52 ライセンス要求/取得部
53 特定利用環境
54-1 利用環境特定物理要素
54-2
54-N
55-1 コンテンツストレージデバイス
55-2
55-M
56-1 再生デバイス
56-2
56-L
57-1 物理要素ID
58-1 暗号化/復号化評価部
59-1 物理要素ID
60-1 暗号化/復号化評価部
61-1 物理要素ID
62-1 暗号化/復号化評価部
S10 秘匿コンテンツ登録
S11 応答
S12 アクセス制御情報登録(コンテンツ復号キー)
S13 応答
S14 ACL設定
S15 応答
S16 秘匿コンテンツ配布要求
S17 秘匿コンテンツ配布
S18 利用要求
S19 物理要素条件指定
S20 物理要素ID証明書群
S21 ライセンス送信

【図２】

図１に示した著作権システム20の内部処理手順を示すフローチャート



【図３】

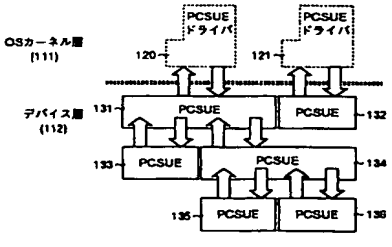
会計条件と物理環境特定要素条件との一例を示す図

会計条件値（Account Condition Value）	利用状況（Usage State）
max Count：操作可能回数最大値	count：操作済回数
max Length：読み出し最大長さ	totalLen：読み出し済長さ＋ 被要求読み出し長さ
max TimeLen：実行可能最大時間	totalTime：実行済時間長
max Debt：借入可能金額（課金条件）	debt：残金（マイナスは借入金額）

物理環境特定要素（PCSUE）条件	物理要素IDクラス（PCSUE-IDClass）
(1) 計算機本体	PSN (プロセッサシリアル番号)
(2) 周辺デバイス	DSN：デバイスの種別、シリアル番号
(3) メディア	MSN：メディアの種別、シリアル番号
(4) ICカード	certificates：ICカードが発行する証明書
(5) 人体部位（指紋、網膜…）	body Parts：人体部位（指紋、網膜…）認証情報
(6) 許可する時間帯	time Period：時刻（ローカルクロック、GPSなど）
(7) ネットワークドメイン	MACAddress：MACアドレス
(8) 地理的位置（利用国など）	location：GPS/PHS検出位置
(9) 人の記憶	user-ID WithPwd：ユーザIDとパスワード
(10) グループ	group：物理要素IDの集合

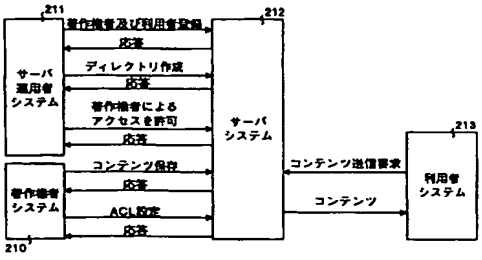
【図９】

包含関係をもった物理要素の一例を示す図



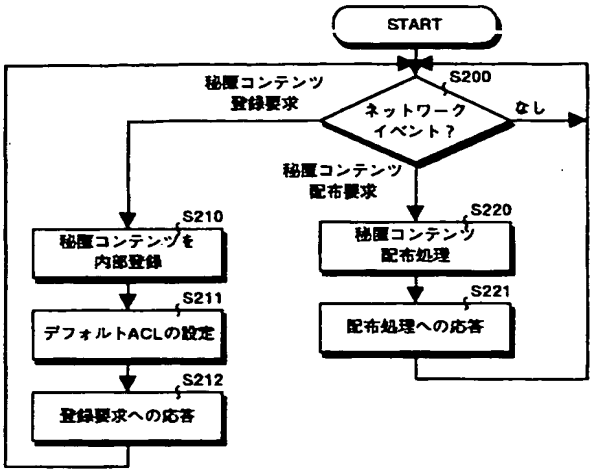
【図１８】

従来のアクセス制御モデルに対応したコンテンツ利用制御システムの概要構成を示す図



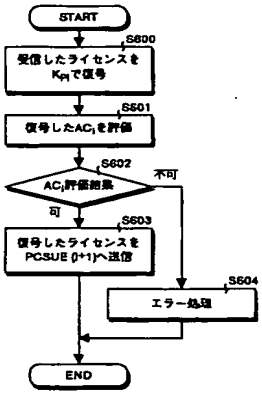
【図４】

図１に示したコンテンツサーバ30の内部処理手順を示すフローチャート



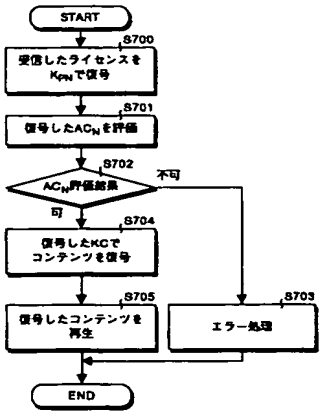
【図１２】

利用者端末特定処理装置によるライセンス復号処理手順を示すフローチャート



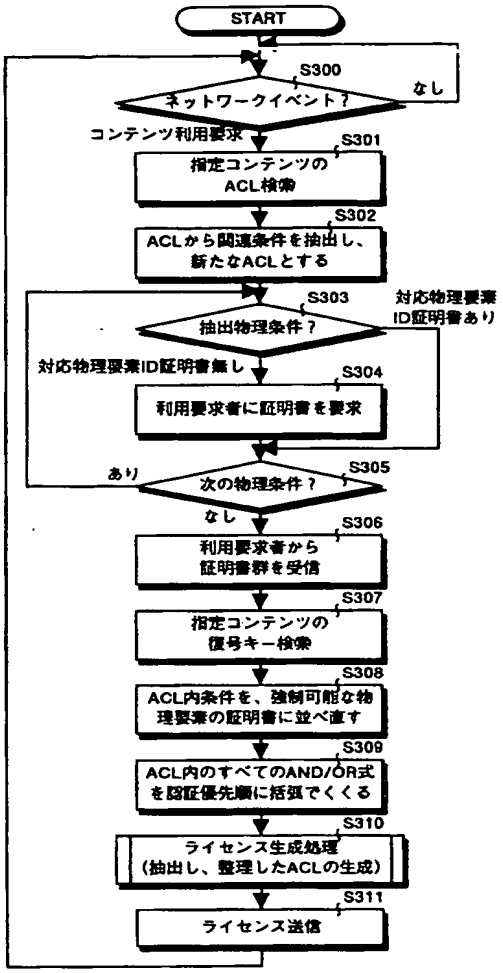
【図１３】

再生デバイスの物理装置によるライセンス復号処理手順を示すフローチャート

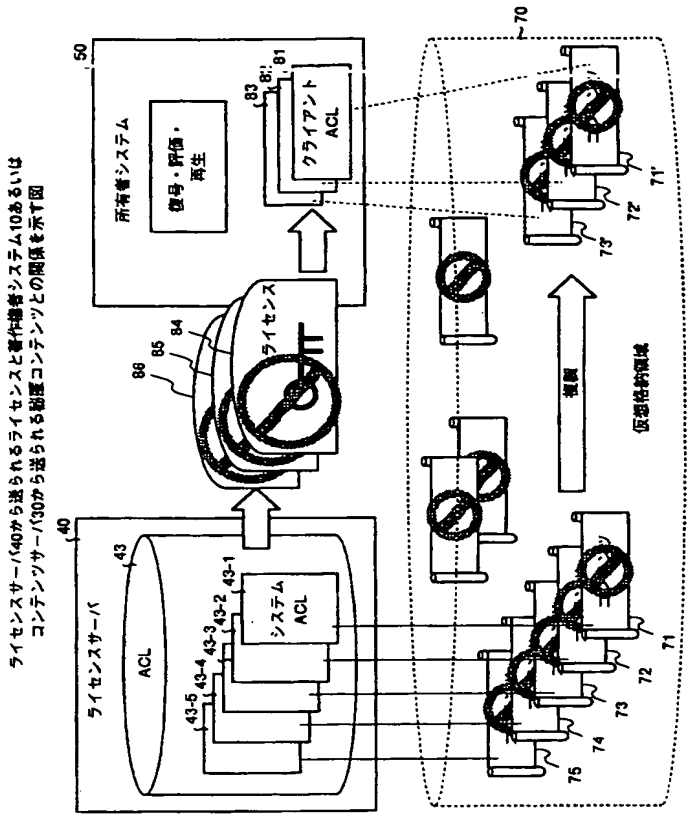


【図５】

図１に示したライセンスサーバ30の内部処理手順を示すフローチャート



【図６】


ライセンスサーバ40から送られるライセンスと著作権者システム10あるいは
コンテンツサーバ30から送られる秘匿コンテンツとの関係を示す図
50
所有者システム
復号・評価・
再生
81
83
クライアント
ACL
ライセンス
84
85
86
40
ライセンスサーバ
43
ACL
43-1
43-2
43-3
43-4
43-5
システム
ACL
70
71'
72'
73'
71
72
73
74
75
複製
仮想格納領域

【図７】

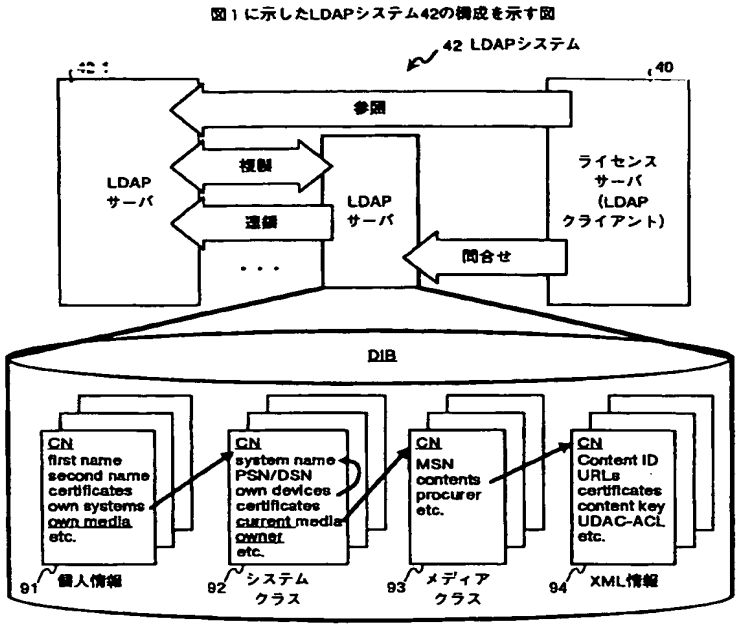
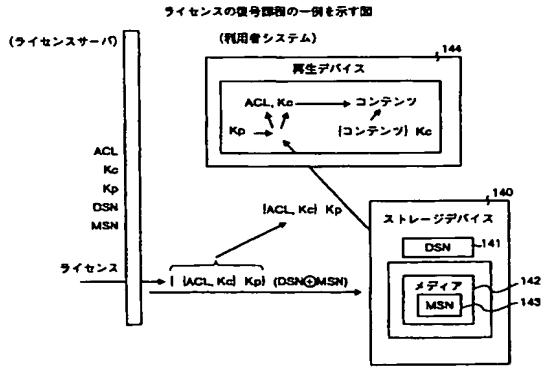
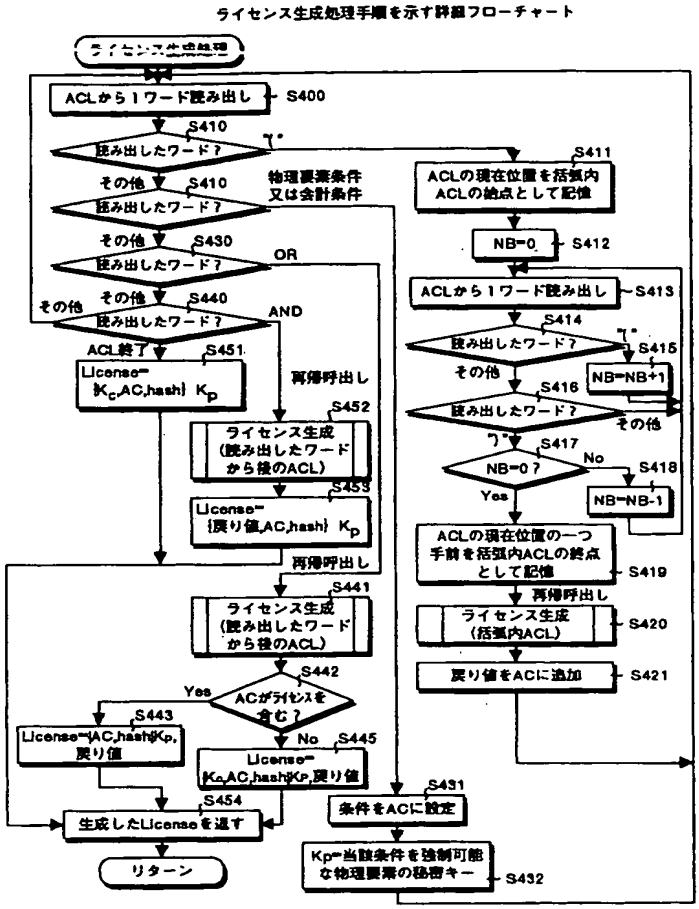


図１に示したLDAPシステム42の構成を示す図
42 LDAPシステム
40
参照
複製
連絡
問合せ
LDAP サーバ
LDAP サーバ
ライセンス サーバ (LDAP クライアント)
DIB
CN
first name
second name
certificates
own systems
own media
etc.
91 個人情報
CN
system name
PSN/DSN
own devices
certificates
current media
owner
etc.
92 システム クラス
CN
MSN
contents
procurer
etc.
93 メディア クラス
CN
Content ID
URLs
certificates
content key
UDAC-ACL
etc.
94 XML情報

【図１４】

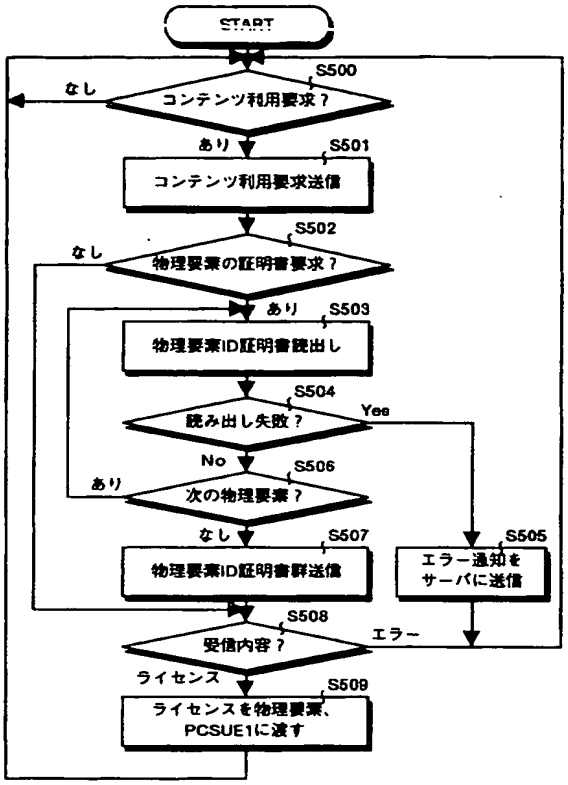

ライセンスの復号課程の一例を示す図
(ライセンスサーバ)
(利用者システム)
144
再生デバイス
ACL, Kc
コンテンツ
Kp
[コンテンツ] Kc
ACL
Kc
Kp
DSN
MSN
ライセンス
[ACL, Kc] Kp
[[ACL, Kc] Kp] (DSN⊕MSN)
140
ストレージデバイス
DSN
141
メディア
MSN
142
143

【図１０】


ライセンス生成処理手順を示す詳細フローチャート
ライセンス生成処理
ACLから１ワード読み出し
S400
S410
読み出したワード？
その他
S410
読み出したワード？
物理要素条件
又は会計条件
その他
S430
読み出したワード？
OR
その他
S440
読み出したワード？
AND
その他
ACL終了
S451
License=
{Kc,AC,hash} Kp
再帰呼出し
S452
ライセンス生成
（読み出したワード
から後のACL）
S453
License=
{戻り値,AC,hash} Kp
再帰呼出し
S441
ライセンス生成
（読み出したワード
から後のACL）
S442
ACがライセンスを
含む？
Yes
S443
License={AC,hash}Kp,
戻り値
No
S445
License=
{Ka,AC,hash}Kp,戻り値
S454
生成したLicenseを返す
リターン
S411
ACLの現在位置を括弧内
ACLの始点として記憶
S412
NB=0
S413
ACLから１ワード読み出し
S414
読み出したワード？
S415
NB=NB+1
その他
S416
読み出したワード？
その他
S417
NB=0？
No
S418
NB=NB-1
Yes
ACLの現在位置の一つ
手前を括弧内ACLの終点
として記憶
S419
再帰呼出し
ライセンス生成
（括弧内ACL）
S420
戻り値をACに追加
S421
S431
条件をACに設定
Kp=当該条件を強制可能
な物理要素の秘密キー
S432

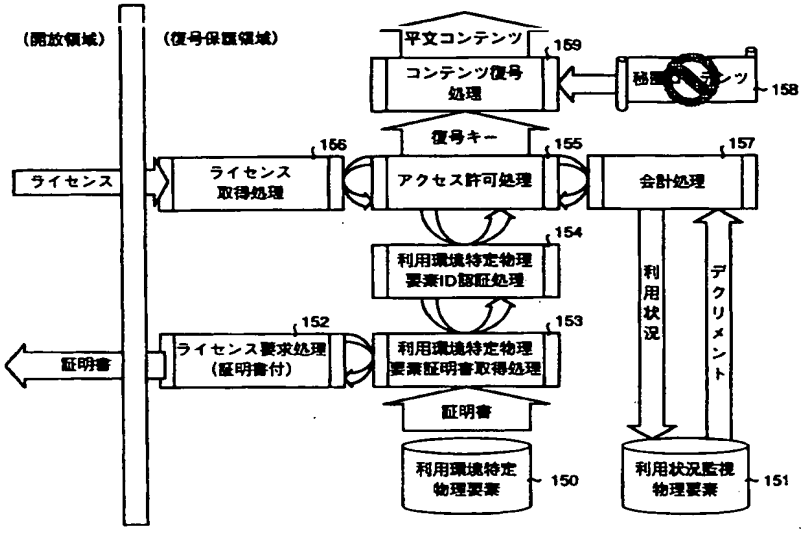
【図１１】

図１に示した利用者システム50の内部処理手順を示すフローチャート



【図１５】

ライセンス要求とライセンス取得によるコンテンツ復号処理を示すデータフロー図



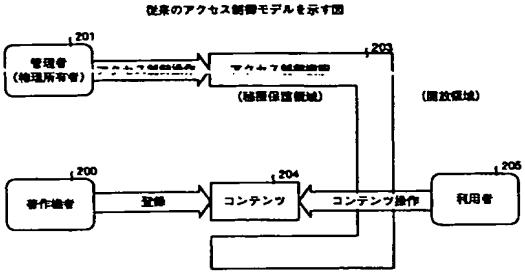
【図１６】

特定利用環境のきエンティティに各処理手続きを実施した場合における保護強度への影響を示す図

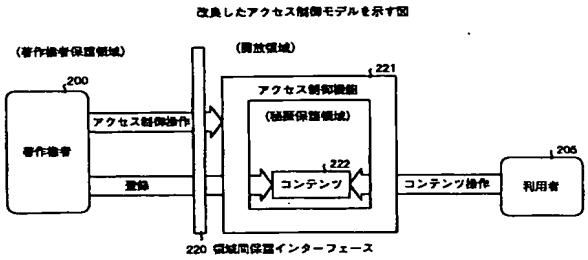
	アプリケーション層	デバイスドライバ層	デバイス層
利用環境特定物理要素所有証明書生成	－	○	◎
利用環境特定物理要素IDSETE	○	－	－
アクセス制御リスト検査	○	－	○
会計情報保護	△	－	◎（ICカード）
条件付アクセス許可	○	－	○
復号	○	－	○

－：実装の意義が少ない　△：危険　○：専門家には保護が弱い　◎：保護が強い

【図１７】


従来のアクセス制御モデルを示す図
201
管理者
(権利所有者)
203
(秘匿保護領域)
(開放領域)
200
著作権者
登録
204
コンテンツ
コンテンツ操作
205
利用者

【図１９】


改良したアクセス制御モデルを示す図
(著作権者保護領域)
(開放領域)
221
アクセス制御機能
(秘匿保護領域)
200
著作権者
アクセス制御操作
登録
222
コンテンツ
コンテンツ操作
205
利用者
220 領域間保護インターフェース

【図２２】

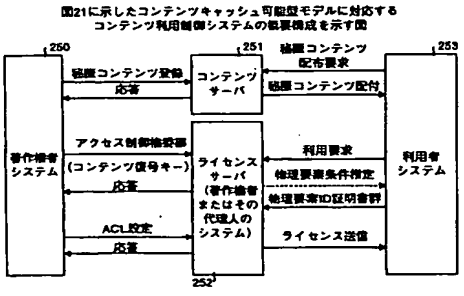
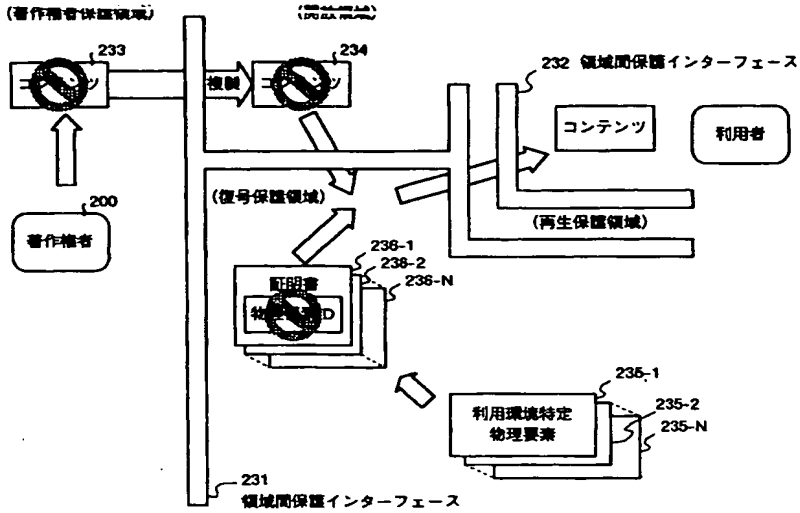


図21に示したコンテンツキャッシュ可能型モデルに対応する
コンテンツ利用制御システムの概要構成を示す図
250
著作権者
システム
秘匿コンテンツ登録
応答
251
コンテンツ
サーバ
秘匿コンテンツ
配布要求
秘匿コンテンツ配付
253
利用者
システム
アクセス制御情報登録
(コンテンツ復号キー)
応答
ライセンス
サーバ
(著作権者
またはその
代理人の
システム)
利用要求
物理要素条件指定
物理要素ID証明書群
ライセンス送信
ACL設定
応答
252

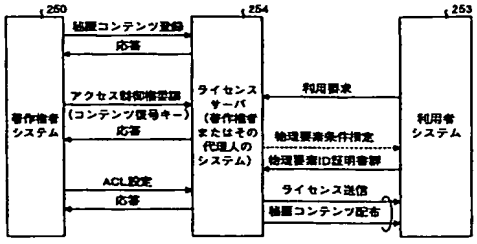
【図２０】

従来のコンテンツ利用制御システムのコンテンツ配布モデルを示す図

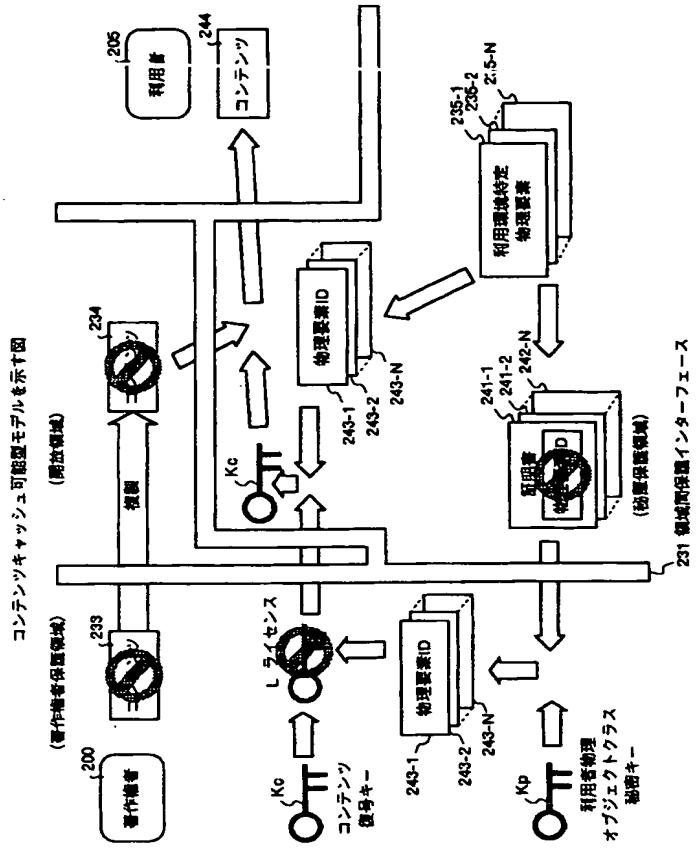


【図２３】

コンテンツ同時配布型モデルを実現するコンテンツ利用制御システム
の概要構成を示す図



【図２１】



フロントページの続き

(72)発明者　宮澤　雄司
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

Ｆターム(参考)　5B017 AA01 AA07 BA05 BA07 BB03
BB10 CA07 CA08 CA09 CA12
CA14 CA15 CA16
5B085 AC03 AE06 AE29

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-293439
(43)Date of publication of application : 20.10.2000

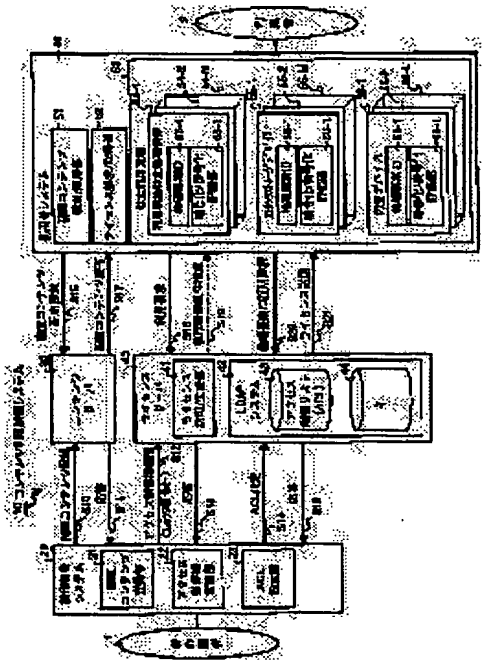
(51)Int.Cl. G06F 12/14
G06F 15/00

(21)Application number : 11-099482
(22)Date of filing : 06.04.1999

(71)Applicant : FUJITSU LTD
(72)Inventor : HATAKEYAMA TAKAHISA
YOSHIOKA MAKOTO
MIYAZAWA YUJI

(54) CONTROL SYSTEM AND DEVICE FOR UTILIZING CONTENT AND COMPUTER READABLE RECORDING MEDIUM WITH PROGRAM MAKING COMPUTER EXECUTE THE UTILIZING METHOD RECORDED THEREON

(57)Abstract:
PROBLEM TO BE SOLVED: To allow a person having information providing authority to perform content use control smoothly and also to prevent the illegal use of a content with high accuracy.
SOLUTION: This system has a copyright holder system 20, a content server 30, a license server 40 and a user system 50, and the ACL setting part 23 of the system 20 sets plural partial use permission conditions to a content as a use permission condition ACL further undergoing structured representation by the combination of OR and AND operations on the basis of the IDs of plural physical elements including media used in the system 50 and a user ID and stores them in an access control list 43. The server 40 controls the use of content by a user 2 by using the list 43, and a condition corresponding to the use situation of the content, for instance, an accounting condition such as the maximum operable number and a charging condition can be set in the access control list.



LEGAL STATUS

[Date of request for examination]	02.11.2000
[Date of sending the examiner's decision of rejection]	21.01.2003
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3471654
[Date of registration]	12.09.2003
[Number of appeal against examiner's decision of rejection]	2003-02729
[Date of requesting appeal against examiner's decision of rejection]	20.02.2003
[Date of extinction of right]	

CLAIMS

[Claim(s)]

[Claim 1] In the contents use control system which performs use control of these contents offered by the information offer authority person including those who were permitted by the information implementer and this information implementer who are an implementer of contents A user means by which a user uses said contents, Further two or more partial use authorization conditions of receiving said contents based on the identification information about the physical element of the user means containing the media used within said user means concerned, and the identification information about said user with the combination of an OR and an AND The contents use control system characterized by having a setting means to set up as use authorization conditions which carried out the structuring expression, and the use control means which controls use of said contents by said user means based on the use authorization conditions set up by said setting means.

[Claim 2] The partial use authorization conditions which said setting means sets up are a contents use control system according to claim 1 characterized by including the accounting conditions which are conditions over the category which changes according to said user means and said user's use situation.

[Claim 3] Said use control means receives the contents use demand from said user means. It has a generation means to generate the consent information enciphered by the identification information about two or more physical elements of the user means containing the media which use said use authorization conditions and the decode key of said contents within said user means concerned. Said user means decodes said consent information sent according to said contents use demand based on the identification information of the physical element by the user means concerned. The contents use control system according to claim 1 or 2 characterized by using the decode key of said contents and decoding said enciphered contents when satisfying

said use authorization conditions.

[Claim 4] Said generation means is a contents use control system according to claim 3 characterized by multiplexing encryption by the identification information of the physical element corresponding to the partial use authorization conditions concerned, and performing it when between the partial use authorization conditions within said use authorization condition is described by the AND.

[Claim 5] Said physical element is the contents use control system of any one publication of claim 1–4 characterized by including the physical element included by other physical elements.

[Claim 6] The contents use control system of any one publication of claim 1–5 characterized by having further the contents server which holds the contents enciphered with said information offer authority person means, receives the contents distribution request from said user means, and sends said enciphered contents to the user means concerned on an open network.

[Claim 7] In the contents use control system which performs use control of these contents offered by the information offer authority person including those who were permitted by the information implementer and this information implementer who are an implementer of contents The user means which decodes the contents which used the decode key of said contents and were enciphered when satisfying the use authorization conditions which decoded the consent demand which performs the use demand of contents and is sent according to the contents use demand concerned based on the identification information of the physical element of the means concerned, and were acquired, Further two or more partial use authorization conditions of receiving said contents based on the identification information about the physical element of the user means containing the media used within said user means concerned, and the identification information about said user with the combination of an OR and an AND A setting means to set up beforehand the use authorization conditions which carried out the structuring expression, and a condition storing means to store the use authorization conditions set up by said setting means, An extract means to receive the use demand of the contents from a maintenance means to hold the decode key of said contents, and said user means, and to extract the use authorization conditions corresponding to the user means concerned, and the decode key of said contents, The contents use control system characterized by having a generation means to generate the consent information which enciphered said use authorization conditions and the decode key of said contents based on the identification information of the physical element sent from said user means, and to

send out to the user means concerned.

[Claim 8] In the contents use equipment with which it connects with a network and a user uses contents A demand means to transmit the identification information about the physical element of the contents use equipment concerned, and the identification information about a user to the contents management equipment which manages contents according to the use demand of contents, A means to decode based on the identification information about the physical element of the contents use equipment concerned, and to ask for use authorization conditions and the decode key of contents from the consent information transmitted by contents management equipment corresponding to the use demand of said contents, Contents use equipment characterized by having the means which uses said decode key for which it asked, and decodes contents when said use authorization conditions searched for are judged and a permission is granted.

[Claim 9] It is the record medium which stored the program performed by computer of the contents use equipment with which it connects with a network and a user uses contents and in which computer reading is possible. The demand process which transmits the identification information about the physical element of the contents use equipment concerned, and the identification information about a user to the contents management equipment which manages contents according to the use demand of contents, The process which decodes based on the identification information about the physical element of the contents use equipment concerned, and asks for use authorization conditions and the decode key of contents from the consent information transmitted by contents management equipment corresponding to the use demand of said contents, The record medium which recorded the program for operating the means which uses said decode key for which it asked, and decodes contents when said use authorization conditions searched for are judged and a permission is granted and in which computer reading is possible.

[Claim 10] A user corresponds to the use demand of said contents in the contents use equipment using contents. A means to decode based on the identification information about the physical element of the contents use equipment concerned, and to ask for use authorization conditions and the decode key of contents from the consent information on contents, Contents use equipment characterized by having the means which uses said decode key for which it asked, and decodes contents when said use authorization conditions searched for are judged and a permission is granted.

[Claim 11] Are the record medium which stored the program which a user performs by computer of the contents use equipment using contents and in which computer

reading is possible, and it corresponds to the use demand of said contents. The process which decodes based on the identification information about the physical element of the contents use equipment concerned, and asks for use authorization conditions and the decode key of contents from the consent information on contents, The record medium which recorded the program for operating the process which uses said decode key for which it asked, and decodes contents when said use authorization conditions searched for are judged and a permission is granted and in which computer reading is possible.

Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the record medium which recorded the program information offer authority persons, such as a copyright person, make [program] a computer perform [program] the contents use control system which controls use of the contents offered through an open network, contents use equipment, and its usage and in which computer reading is possible.

[0002] A monetary role provides people with fair remuneration with the property as matter called the money. As for an object called money, it was indispensable requirements not a mere verbal agreement-share concept but for forgery [further / exist physically, can carry and / in addition to a publishing agency] to be difficult. It existed physically, and by being portable, it could check impartially by the users of the value, and fair money issue-origin was able to control the opportunity of the fair check by counterfeit difficulty. However, the day when now monetary forged difficulty will collapse by development of a technology in recent years is near. The new value check object replaced with money is needed. It is necessary to exist physically too first, and the object can be carried and needs to be difficult to forge. Furthermore, the object carries out the access control of the publishing agency.

[0003] In addition to the demand from this security strengthening side, the demand of implementation of a "superdistribution" is also increasing from the side face of diversification of the distribution of information, large-capacity-izing, and improvement in the speed. The environment which realized this "superdistribution" satisfies the following conditions. that (1) information user can obtain digital information for free mostly, that the conditions on which (2) information providers specified the conditions (accounting, alteration use conditions, etc.) to which use of that information is permitted, and the user has agreed can be forced, and (3) -- in using this service, a required information user's add operation is "check of access condition" extent -- it comes out. [namely,]

[0004] It is expectable that accuracy and the system which can be performed safely contribute the access control of such a superdistribution also to unfair correction of royalty collection, such as a charge of a license. the present system -- a work -- about -- although a provider cannot gain profits unless it can sell a number, to be able to build a system so that it may cross to a copyright person's hand correctly is desired. Moreover, the remuneration corresponding to each one of service charges is wanted to be distributed impartially until it results [from an expert-artist] in the designer who offers creation as components.

[0005]

[Description of the Prior Art] When access to contents, such as a work, was conventionally controlled on a distributed-system environment, especially an open network, use of contents was controlled by storing contents in the server which can be accessed from the user of contents, and controlling access to this server. Here, contents are digital contents with the structure recordable on a single store medium as a set of a bit string, and a document text, an image, an animation, program software, etc. are included.

[0006] For example, drawing 17 is drawing showing the conventional access-control model. In drawing 17 , contents 204 are enabling contents actuation from a user 205 through the access-control function 203. Moreover, for example, the copyright person 200 was taken care of by the access-control function 203 in contents 204, it is only registering with a server and the access-control actuation to the access-control function 203 was made by persons other than copyright person 200, for example, the manager who manages this server.

[0007] That is, it is managed by the server employment person system 211 in which management employment is done by the manager 201, and the server employment person system 211 performs a copyright person and a user registration to the server system 212, and the server system 212 which holds contents as shown in drawing 18 performs directory generation for it, and also performs permitting the access control by the copyright person further. The copyright person system 210 makes the contents of a copyright person's work save in the server system 212, and sets up access-control conditions (ACL) to the server system 212. In this case, a copyright person has to get authorization of an access control to the server system 212. On the other hand, the user system 213 acquires the contents saved in the server system 212, when performing a contents Request to Send to the server system 212 and satisfying ACL on the occasion of use of contents.

[0008] However, if all authority is granted to the user of contents and a user changes by

migration or the copy (duplicate), to the contents of migration or a copy place, the authority of the copyright person of a basis will not be committed at all. Moreover, between the server manager who saves a contents object, and the copyright person, the state of access consent compulsion to an object is not clear, either, for example, a copyright person does not refuse and have a server manager, and to be able to change an access privilege was made into the natural thing.

[0009] On the other hand, without the distributed-system environment's having been promoted by low-pricing of a storage in recent years etc., and network traffic concentrating by it, the cache of the contents can be carried out to two or more servers, it can distribute now, and access to a contents object could be performed at the high speed. Therefore, although the access-control model as shown in drawing 17 should just build the firm access-control function only to the entry to the contents actuation by the user 205, it needed to perform all the directions-access control or security protection under the distributed-system environment mentioned above.

[0010] Then, the access-control model as shown in drawing 19 was able to be considered. The copyright person 200 is separated into the copyright person protected area which is a field which can be protected, the open field which receives the attack from all the outside, and protection of an alteration of hard/software and the secrecy protected area to which digital data duplicate prevention processing is performed by the conventional security technique in this access-control model. A secrecy protected area is protected by the omnidirection access-control function 221, and contents 222 are saved in this access-control function 221.

[0011] The copyright person 200 is also enabling access-control actuation to the access-control function 221 with registration of contents 222 to these contents. A user 205 will acquire contents 222 from an open field through the access-control function 221. In addition, the field protection interface 220 is an interface which performs protection between a copyright person protected area and an open field.

[0012] Somatization of the access-control model under the distributed-system environment shown in this drawing 19 is indicated by the U.S. Pat. No. 5339433 number official report, and the technique of checking a user's device in JP,9-134311,A, a U.S. Pat. No. 5392351 number official report, a U.S. Pat. No. 5555304 number official report, and a U.S. Pat. No. 5796824 number official report, and preventing unjust use of contents in them is indicated. Hereafter, the conventional contents use control system is explained with reference to these official reports.

[0013] Drawing 20 is drawing showing the contents distribution model of the conventional contents use control system. In drawing 20 , it is equivalent to the secrecy

protected area indicated to be a decode protected area and a playback protected area to drawing 18 , a decode protected area is a field of protection of an alteration of hard/software, and duplicate prevention protection of output data, and a playback protected area is a field of duplicate prevention of digital decode data. The use environmental specification physical element (PCSUE) 235-1 · 235-N are physical elements which specify the use environment of contents, and, specifically, are CPU, a peripheral device, a removable storage, an IC card, etc.

[0014] In a decode protected area, the contents 234 which are the duplicates of the contents 233 enciphered by the copyright person 200, and exist in the server of an open field are decoded based on the certificate 236-1 of the physical element ID corresponding to PCSUE 235-1 · 235-N · 236-N, and these compounded contents are used for a user through a playback protected area. Therefore, contents are enciphered by the key corresponding to a physical element ID (contents 233), and in order to decode the contents 234 corresponding to these contents 233, each physical element ID or the secret key corresponding to it is needed.

[0015] A license has the contents cache possible mold model acquired to another timing by saving the contents enciphered as the license coincidence model which distributes the license used for a contents distribution model here in order to decode the enciphered contents to the enciphered contents and coincidence into the cache of a server. Drawing 21 is drawing showing this contents cache possible mold model.

[0016] In drawing 21 , first, it is a copyright person protected area, and an author 200 generates contents and enciphers these contents, after that, he reproduces and a cache is done to the server of an open field etc. On the other hand, the certificate 241-1 which enciphered the physical element ID of PCSUE 235-1 · 235-N · 241-N It is outputted to a copyright person protected area in the condition of having been enciphered, and a secret key Kp is taken out from the user physics object class corresponding to PCSUE 235-1 · 235-N. This secret key Kp, and a certificate 241-1 · 241-N to a physical element ID 243-1 · 243-N are decoded, and by this physical element ID 243-1 · 243-N, the contents decode key Kc is enciphered and it outputs to a security field.

[0017] In a security field, the enciphered contents decode key Kc is decoded by the physical element ID 242-1 · 242-N, and the contents decode key Kc is obtained. The enciphered contents 234 which are acquired from an open field using this contents decode key Kc are decoded, and a user 205 is made to use as contents 244.

[0018] Drawing 22 is the block diagram showing the outline configuration of the contents use control system corresponding to the contents cache possible mold model shown in drawing 21 . In drawing 22 , the copyright person system 250 exists in a

copyright person protected area, the contents server 251 exists in an open field, and a license server 252 and the user system 253 exist in a secrecy protected area. The copyright person system 250 enciphers the created contents, and saves these enciphered secrecy contents at the contents server 251.

[0019] Moreover, the contents decode key Kc is transmitted to a license server 252, and the transfer of the right of an access control is performed to a license server 252. Furthermore, an access control list (ACL) setup is performed. When the use demand which shows that contents are used is transmitted to a license server 252 and the certification group of a physical element ID is not attached at this time, by the physical element criteria specification of a license server 252, the user system 253 acquires the certification group of a physical element ID, and sends it out to a license server 252.

[0020] A license server 252 acquires the secret key Kp of a user's physical object class, as shown in drawing 21 , and the contents decode key Kc enciphered with the physical element ID which decoded and decoded the physical element ID certification group is sent out to the user system 253 as license L. If the physical element ID of the user system 253 is in agreement, decode is performed by this and secrecy contents can be decoded by it using this decoded contents decode key Kc.

[0021] In addition, since secret contents are saved at the contents server 251, the user system 253 needs to perform a secret contents distribution request to the contents server 251 separately, and needs to receive distribution of secret contents from the contents server 251.

[0022] On the other hand, drawing 23 shows the outline configuration block Fig. of the contents use control system which realizes a contents coincidence distribution mold model. In drawing 23 , the contents server 251 will not exist but it will be sent to the user system 253 at license transmission and coincidence. Since secret contents are beforehand carried to the server near the user system 253 in time when acquiring secret contents through the contents server 251 as shown in drawing 22 , the user system 253 should just carry out a use demand, when contents are required.

[0023] Moreover, suitable selection of the distribution channel of contents is attained as compared with a contents coincidence distribution mold model, and compaction of the response time can be expected on the occasion of contents acquisition for a user. Moreover, it is possible to distribute contents beforehand with the cache by the ROM medium base, broadcast, and the Proxy server etc. apart from offer of a license in a contents cache possible mold model, and there are many advantages.

[0024]

[Problem(s) to be Solved by the Invention] However, although secrecy contents can be

decoded fundamentally and these contents can be used in the conventional contents use control system mentioned above if it is equipment which is in agreement with a user system at the physical element ID of a proper Since this physical element ID is generating the license (use authorization conditions) For example, the conditions which restrict the count of read-out of the contents determined with a copyright person's intention could not be added, a time limit could not be prepared, accounting conditions could not be set up, but there was a trouble that flexible contents use control could not be performed.

[0025] Moreover, it did not restrict having always simple composition, but when it was a device with a complicated configuration, a use environmental specification physical element may have inaccurate specific device or specific components of the device, and even if it generated use authorization conditions with the use environmental specification physical element which is the device of an only big configuration, in such a case, there was a trouble overlooking injustice and that security fell.

[0026] while, as for this invention, an information offer authority person including those who were made in view of the above and permitted by information implementers, such as a copyright person, can perform contents use control flexibly -- the unjust use of contents -- precision -- it aims at offering the record medium which recorded the program which makes a computer perform the contents use control system which can be prevented highly, contents use equipment, and its usage and in which computer reading is possible.

[0027]

[Means for Solving the Problem] In order to attain the above-mentioned purpose, invention concerning claim 1 In the contents use control system which performs use control of these contents offered by the information offer authority person including those who were permitted by the information implementer and this information implementer who are an implementer of contents A user means by which a user uses said contents (50 of drawing 1), Further two or more partial use authorization conditions of receiving said contents based on the identification information about the physical element of the user means containing the media used within said user means concerned, and the identification information about said user with the combination of an OR and an AND It is characterized by having a setting means (23 of drawing 1) to set up as use authorization conditions which carried out the structuring expression, and the use control means (40 of drawing 1) which controls use of said contents by said user means based on the use authorization conditions set up by said setting means.

[0028] According to invention concerning this claim 1, a setting means Further two or

more partial use authorization conditions of receiving said contents based on the identification information about the physical element of the user means containing the media used within said user means concerned, and the identification information about said user with the combination of an OR and an AND Setting up as use authorization conditions which carried out the structuring expression, said use control means controls use of said contents by said user means based on the use authorization conditions set up by said setting means, and enables flexible use control based on use authorization conditions.

[0029] Moreover, the partial use authorization conditions that said setting means sets up invention concerning claim 2 in a contents use control system according to claim 1 are characterized by including the accounting conditions (equivalent to the accounting condition value of drawing 3) which are conditions over the category which changes according to said user means and said user's use situation.

[0030] according to invention concerning this claim 2 -- a setting means -- it is made for the partial use authorization conditions set up to include the accounting conditions which are conditions over the category which changes according to said user means and said user's use situation, and they can perform use control to a user finely further.

[0031] Invention concerning claim 3 is set to a contents use control system according to claim 1 or 2. Moreover, said use control means (40 of drawing 1) The contents use demand (S18 of drawing 1) from said user means (50 of drawing 1) is received. It has a generation means (41 of drawing 1) to generate the consent information enciphered by the identification information about two or more physical elements of the user means containing the media which use said use authorization conditions and the decode key of said contents within said user means concerned. Said user means decodes said consent information sent according to said contents use demand based on the identification information of the physical element by the user means concerned. When satisfying said use authorization conditions, it is characterized by using the decode key of said contents and decoding said enciphered contents.

[0032] According to invention concerning this claim 3, a generation means receives the contents use demand from said user means. The consent information enciphered by the identification information about two or more physical elements of the user means containing the media which use said use authorization conditions and the decode key of said contents within said user means concerned is generated. Said user means decodes said consent information sent according to said contents use demand based on the identification information of the physical element by the user means concerned, and when satisfying said use authorization conditions, the decode key of said contents is

used for it, and it decodes said enciphered contents.

[0033] Moreover, it is characterized by said generation means (41 of drawing 1) performing invention concerning claim 4 in the contents use control system of claim 3, by multiplexing encryption by the identification information of the physical element corresponding to the partial use authorization conditions concerned, when between the partial use authorization conditions within said use authorization condition is described by the AND (equivalent to several 1 and several 2).

[0034] According to invention concerning this claim 4, when between the partial use authorization conditions within a use authorization condition is described by the AND, it can carry out by the ability multiplexing encryption by the identification information of the physical element corresponding to the partial use authorization conditions concerned, and the danger of the theft of the contents decode key by attack success to some physical elements can be distributed.

[0035] Moreover, invention concerning claim 5 is characterized by said physical element containing the physical element (131-136 of drawing 9) included by other physical elements in a contents use control system according to claim 1 to 4.

[0036] According to invention concerning this claim 5, even if a physical element is a physical element in inclusion relation, it can be dealt with as one physical element, and the injustice of this one physical element cannot be allowed, either, but the danger of calling it the theft of a contents decode key can be distributed.

[0037] Moreover, invention concerning claim 6 is characterized by having further the contents server (30 of drawing 1) which holds the contents enciphered with said information offer authority person means on the open network, receives the contents distribution request from said user means, and sends said enciphered contents to the user means concerned in a contents use control system according to claim 1 to 5.

[0038] Since it has the contents server which holds the contents enciphered with said information offer authority person means, receives the contents distribution request from said user means, and sends said enciphered contents to the user means concerned on an open network according to invention concerning this claim 6, an open network can fully be utilized, the congestion of the traffic in the system concerned can be prevented, and contents can be gained quickly.

[0039] Moreover, invention concerning claim 7 performs the use demand of contents in the contents use control system which performs use control of these contents offered by the information offer authority person including those who were permitted by the information implementer and this information implementer who are an implementer of contents. The user means which decodes the contents which used the decode key of said

contents and were enciphered when satisfying the use authorization conditions which decoded the consent demand sent according to the contents use demand concerned based on the identification information of the physical element of the means concerned, and were acquired (50 of drawing 1), Further two or more partial use authorization conditions of receiving said contents based on the identification information about the physical element of the user means containing the media used within said user means concerned, and the identification information about said user with the combination of an OR and an AND A setting means to set up beforehand the use authorization conditions which carried out the structuring expression (23 of drawing 1), A condition storing means to store the use authorization conditions set up by said setting means (43 of drawing 1), An extract means to receive the use demand of the contents from a maintenance means (44 of drawing 1) to hold the decode key of said contents, and said user means, and to extract the use authorization conditions corresponding to the user means concerned, and the decode key of said contents (drawing 42), It is characterized by having a generation means (41 of drawing 1) to generate the consent information which enciphered said use authorization conditions and the decode key of said contents based on the identification information of the physical element sent from said user means, and to send out to the user means concerned.

[0040] According to invention concerning this claim 7, a setting means Further two or more partial use authorization conditions of receiving said contents based on the identification information about the physical element of the user means containing the media used within a user means concerned, and the identification information about said user with the combination of an OR and an AND While setting up beforehand by storing in the condition storing means within said use control means the use authorization conditions which carried out the structuring expression, the decode key of said contents is held for a maintenance means. An extract means receives the use demand of the contents from said user means, extracts the use authorization conditions corresponding to the user means concerned, and the decode key of said contents, generates the consent information which enciphered said use authorization conditions and the decode key of said contents based on the identification information of the physical element sent from said user means, and sends it out to the user means concerned. A user means decodes said consent information sent according to said contents use demand based on the identification information of the physical element by the user means concerned, and when satisfying said use authorization conditions, the decode key of said contents is used for it, and it decodes said enciphered contents.

[0041] Moreover, invention concerning claim 8 is set to the contents use equipment with

which it connects with a network and a user uses contents. A demand means to transmit the identification information about the physical element of the contents use equipment concerned, and the identification information about a user to the contents management equipment which manages contents according to the use demand of contents (52 of drawing 1), From the consent information transmitted by contents management equipment corresponding to the use demand of said contents A means to decode based on the identification information about the physical element of the contents use equipment concerned, and to ask for use authorization conditions and the decode key of contents (58-1 of drawing 1 , 60-1, 62-1), When said use authorization conditions searched for are judged and a permission is granted, it is characterized by having the means (51 of drawing 1) which uses said decode key for which it asked, and decodes contents.

[0042] According to invention concerning this claim 8, a demand means accepts the use demand of contents. If the identification information about the physical element of the contents use equipment concerned and the identification information about a user are transmitted to the contents management equipment which manages contents then, from the consent information transmitted by contents management equipment corresponding to the use demand of said contents Protection reinforcement is made high, as it decodes based on the identification information about the physical element of the contents use equipment concerned, and it asks for use authorization conditions and the decode key of contents, and said decode key for which it asked is used and contents are decoded, when said use authorization conditions searched for are judged and a permission is granted.

[0043] Moreover, invention concerning claim 9 is a record medium which stored the program performed by computer of the contents use equipment with which it connects with a network and a user uses contents and in which computer reading is possible. The demand process which transmits the identification information about the physical element of the contents use equipment concerned, and the identification information about a user to the contents management equipment which manages contents according to the use demand of contents (S501 of drawing 11), From the consent information transmitted by contents management equipment corresponding to the use demand of said contents The process which decodes based on the identification information about the physical element of the contents use equipment concerned, and asks for use authorization conditions and the decode key of contents (S600 and S601 of drawing 12 , S700, S701 of drawing 13), When said use authorization conditions searched for are judged and a permission is granted, it is the record medium which recorded the program

for operating the process (S704 of drawing 13) which uses said decode key for which it asked, and decodes contents and in which computer reading is possible.

[0044] According to invention concerning this claim 9, the use demand of contents is first accepted according to a demand process. The identification information about the physical element of the contents use equipment concerned and the identification information about a user are transmitted to the contents management equipment which manages contents. then, from the consent information transmitted by contents management equipment corresponding to the use demand of said contents Decode based on the identification information about the physical element of the contents use equipment concerned, and it asks for use authorization conditions and the decode key of contents. Then, protection reinforcement is made high, as said decode key for which it asked is used and contents are decoded, when said use authorization conditions searched for are judged and a permission is granted.

[0045] Moreover, invention concerning claim 10 is set to the contents use equipment with which a user uses contents. It corresponds to the use demand of said contents. From the consent information on contents A means to decode based on the identification information about the physical element of the contents use equipment concerned, and to ask for use authorization conditions and the decode key of contents (58-1 of drawing 1 , 60-1, 62-1), When said use authorization conditions searched for are judged and a permission is granted, it is characterized by having the means (51 of drawing 1) which uses said decode key for which it asked, and decodes contents.

[0046] When according to invention concerning this claim 10 it decodes based on the identification information about the physical element of the contents use equipment concerned, and use authorization conditions and the decode key of contents are asked, and said use authorization conditions searched for are judged after that and a permission is first granted from the consent information on contents corresponding to the use demand of contents, protection reinforcement is made high, as said decode key for which it asked is used and contents are decoded.

[0047] Moreover, invention concerning claim 11 is a record medium which stored the program which a user performs by computer of the contents use equipment using contents and in which computer reading is possible. It corresponds to the use demand of said contents. From the consent information on contents The process which decodes based on the identification information about the physical element of the contents use equipment concerned, and asks for use authorization conditions and the decode key of contents (S600 and S601 of drawing 12 , S700, S701 of drawing 13), When said use authorization conditions searched for are judged and a permission is granted, it is the

record medium which recorded the program for operating the process (S704 of drawing 13) which uses said decode key for which it asked, and decodes contents and in which computer reading is possible.

[0048] When according to invention concerning this claim 11 it decodes based on the identification information about the physical element of the contents use equipment concerned, and use authorization conditions and the decode key of contents are asked, and said use authorization conditions searched for are judged after that and a permission is first granted from the consent information on contents corresponding to the use demand of said contents, protection reinforcement is made high, as said decode key for which it asked is used and contents are decoded.

[0049]

[Embodiment of the Invention] The gestalt of suitable operation of the record medium which recorded the program which makes a computer perform the contents use control system applied to this invention with reference to an accompanying drawing below, contents use equipment, and its usage and in which computer reading is possible is explained.

[0050] Drawing 1 is drawing showing the configuration of the contents use control system which is the gestalt of 1 operation of this invention. The contents use control system 10 shown in drawing 1 is a system which controls this use, when a user 2 uses the contents of the work which the copyright person 1 created. In drawing 1 , this contents use control system 10 is large, and has the copyright person system 20, the contents server 30, a license server 40, and the user system 50.

[0051] The copyright person system 20 enciphers the created contents. By sending out a contents decode key required decoding the secrecy contents registration section 21 which performs processing (S10) which registers these enciphered secrecy contents into the contents server 30, and the enciphered contents (secrecy contents) to a license server 40 It has the right transfer section 22 of an access control which performs processing (S12) which transfers the right of an access control to a license server, and the ACL (S14) setting section 23 which sets use authorization conditions (ACL) as a license server 40, and the use control about the contents of a work is managed.

[0052] When the secrecy contents sent from the copyright person system 20 are registered and there is a secrecy contents distribution request from the user system 50 (S16), the contents server 30 is sent out to the user system 50, where these secrecy contents registered and saved are enciphered (S17).

[0053] A license server 40 has license authorization / generation section 41 and the LDAP system 42. License authorization / generation section 41 searches the decode key

corresponding to the physical element ID certificate and this which were added to this use demand when there was a use demand of contents from the user system 50 (S18) from the LDAP system 42, a physical element ID decodes, the contents decode key corresponding to the contents by which the use demand was carried out searches, and the license enciphered with the physical element ID in this searched contents decode key transmits (S21).

[0054] This license is physical environmental specification element conditions, is made equivalent to the structure of a physical element, and serves as an OR and a gestalt of the combination structured using the AND. Moreover, with the gestalt of this operation, not only the physical environmental specification element conditions of having been used from the former but the accounting conditions on condition of a user's use situation are collectively enciphered as ACL. About encryption and a decryption of this license, it mentions later. In addition, when the physical element ID certificate is not added to a use demand (S18), in not existing in the LDAP system 42, physical element criteria specification (S19) is sent to the user system 50, and it returns the physical element ID certificate group which the user system 50 generated (S20).

[0055] On the other hand, when the contents decode key by the right transfer of an access control has been sent from the copyright person system 20 (S12), the database of the key 44 in the LDAP system 42 which mentions this contents decode key later is made to correspond to secrecy contents, and it registers with it. Moreover, this ACL is made that an ACL setup has been sent from the copyright person system 20 (S14), and to correspond to secrecy contents, and it stores in the access control list (ACL) in the LDAP system 42.

[0056] The user system 50 has the distribution request (S16) of secrecy contents, secrecy contents demand / acquisition section 51 which acquires the distributed secrecy contents, a demand (S18) of a license, i.e., a use demand, and license demand / acquisition section 52 which processes acquisition (S21) of a license, and the specific use environment (SUE) 53 of a user system. In the specific use environment 53, a specific contents use environment is said and synthetic information, such as CPU, a peripheral device, a RIMUBARU storage, an IC card, and a contents use situation, is said.

[0057] By the specific use environment, it has the use environmental specification physical elements (PCSUE) 54-1, such as CPU, - 54-N, the contents storage device 55-1 which stores contents - 55-M, and the playback devices 56-1, such as a player and a viewer, - 56-L. Each PCSUE 54-1 - 54-N, each contents storage device 55-1 - 55-M, and each playback device 56-1 - 56-L have encryption / decryption / evaluation section 58-1 - 58-N, 60-1 - 60-M, and 62-1 - 62-L while having each physical element ID 57-1 - 57-N,

59-1 - 59-M, and 61-1 - 61-L.

[0058] When enciphering and outputting with the physical element ID of a self-physical element in enciphering each physical element, and decrypting each physical element, encryption / decryption / evaluation section 58-1 - 58-N, 60-1 - 60-M, and 62-1 - 62-L decrypt with the physical element ID of a self-physical element, and performs processing which evaluates a decode result further. That is, about processing of each physical element ID, it carries out for every physical element, and even if it is on the interface between physical elements, he is trying for information not to leak.

[0059] Processing of the copyright person system 20 mentioned above next, the contents server 30, a license server 40, and a user system of operation is explained mainly with reference to a flow chart. First, with reference to the flow chart of drawing 2 , the internal-processing procedure of the copyright person system 20 is explained.

[0060] In drawing 2 , it judges whether the actuation event generated the copyright person system 20 first (step S100). when the actuation event has not occurred (step S100 -- nothing), this processing is repeated until an actuation event occurs, and the contents of actuation of an actuation event judge secrecy contents registration, ACL registration, and the right transfer of an access control for the actuation event to have occurred (step S100 -- it is) (step S101).

[0061] When the contents of actuation are secrecy contents registration (step 101, secrecy contents registration), the secrecy contents registration section 21 enciphers contents (step S110), specifies the desired contents server 30 from a contents server list (step S111), and performs a secrecy contents registration demand to this specified contents server 30 (step S112). Then, the response from the contents server 30 is obtained and it judges whether the response is O.K. or it is an error (step S113).

[0062] When the response from the contents server 30 is O.K., in being an error, after performing error processing (step S114), it judges further whether the following contents server was specified as it is (step S115). when the processing which shifted to step S112 and was mentioned above when the following contents server was specified (step S115 -- it is) is repeated and the following contents server is not specified (step S115 -- nothing), the processing which shifted to step S100 and was mentioned above is repeated.

[0063] in judging whether the contents decode key as which the ACL setting section 23 was specified further is registered when the contents of actuation are ACL setup (step 101, ACL setup) (step S120), and not registering a contents decode key (step S120 -- nothing), error processing is performed (step S124), and it shifts to step S100 and repeats the processing mentioned above. on the other hand, when there is registration

of a contents decode key (step S120 -- it is), an ACL setting demand is transmitted to a license server 40 (step S122), an ACL registration result is received from a license server 40 (step S123), and the processing which shifted to step S100 after that, and was mentioned above is repeated.

[0064] Moreover, when the contents of actuation are the right transfers of an access control (step S101, right transfer of an access control), the enciphered contents decode key is transmitted to a license server 40 (step S130), the registration result of an encryption contents decode key is received (step S131), it shifts to step S100 and the processing mentioned above is repeated.

[0065] Below, ACL set up by the ACL setting section 23 is explained here. Drawing 3 is drawing showing an example of an access condition, and an access condition has two kinds such as accounting conditions and physical environmental specification element (PCSUE) conditions. As shown in drawing 3 , as accounting conditions which are one of the descriptions of this invention, first, there is maxCount (count maximum of operational) and the use situation of the contents corresponding to this is count (operated count). It is going to access control, i.e., limitation, and license by preparing the limit of the count maximum of operational to the adjustable value of an operated count.

[0066] The use situation of the contents corresponding to the accounting condition value of the next maxLength (read-out length between couplings) is totalLen (asked [read die-length +] read-out die length), and tends to control access by the read-out maximum length of contents. The use situation of the contents corresponding to the accounting condition value of the next maxTimeLen (the maximum time amount which can be performed) is totalTime (performed time amount length), and tends to control access by the maximum time amount of contents which can be performed. The use situation of the contents corresponding to the accounting condition value of the next maxDebt (lease possible amount of money (accounting conditions)) is debt (balance), and the minus value of the balance tends to serve as a debt frame, and tends to control access by accounting conditions.

[0067] Moreover, as physical environmental specification element conditions, there is a body of a computer first, and the class of the physical element ID corresponding to this is PSN, and is the serial number of a processor. Here, a class is an object class on a database. The class of the physical element ID corresponding to the following peripheral device is DSN, and shows the class and serial number of a device. The class of the physical element ID corresponding to the following media is MSN, and shows the class and serial number of media. The physical element ID corresponding to the following IC

card is certificates, and shows the certificate which an IC card publishes.

[0068] The next body parts are a fingerprint and retina (iris) information, and the class of the physical element ID corresponding to this is bodyParts, and is the authentication information on a body part. The class of the physical element ID corresponding to the time zone which the next permits is timePeriod, and are a local clock and global GPS time of day. The next network domain shows the area on a network, and the class of the physical element ID corresponding to this is MACAddress, and shows a MAC Address. The geographical location of the following shows a use country etc., and the class of the physical element ID corresponding to this is location, and shows the location which GPS or PHS detects. The class of the physical element ID corresponding to storage of the next man is user-ID WithPwd, and shows user ID and a password. The class of the physical element ID corresponding to the last group is group, and shows the set of a physical element ID.

[0069] Such an access condition is set up as a set with a logical combination of AND and OR, i.e., ACL. Although there are accounting conditions and physical environmental specification element conditions in an access condition as mentioned above, combination is possible for these to arbitration. For example, the following is set up as one ACL. That is, ACL like udac#aclread:(grop=sysrapOR group=soft4soft) (AND45661244<MSN<45661412) OR count<1;modify:user=yujiOR user=hataORIC#card=1afd234fe4def458c3bac78497bbda6 f;print:group=sysrap; can be set up.

[0070] According to this set-up ACL, "read" shows perusal conditions, and a group is "sysrap" or "soft4soft", and it becomes the conditions for perusal that media serial number MSN exceeds 45661244, and is less than 45661412, or an operated count does not use contents less than one, i.e., once. Furthermore, "modify" shows updating conditions and it becomes the conditions for renewal of contents that a user name is "yuji" or "hata", or the number of "IC#card" is "1afd234fe4def458c3bac78497bbda6f."

[0071] Moreover, "print" can show printout conditions, and a group can restrict it to "sysrap", and it can print contents. The copyright person 1 can set such ACL as arbitration from the copyright person system 20. Operability of this ACL setup improves by using GUI. In addition, you may make it set up the type of ACL with an actuation name. For example, conditions can be chosen access condition (1) Coming [the actuation name 1], and you may enable it to choose conditions access condition (2) Coming [the actuation name 2]. Thereby, operability improves further.

[0072] Below, with reference to the flow chart shown in drawing 4 , the internal-processing procedure of the contents server 30 is explained. In drawing 4 , first,

the contents server 30 judges a secrecy contents registration demand and a secrecy contents distribution request, when a network event is inputted or it is inputted (step S200). when a network event is not inputted (step S200 -- nothing), the decision processing in step 200 is repeated.

[0073] When a network event is a secrecy contents registration demand (step S200, secrecy contents registration demand), internal registration of these secrecy contents by which the registration demand was carried out is carried out (step S210), and default ACL is set up (step S211). And the processing which performed the response to this secrecy contents registration demand (step S212), shifted at step S200, and was mentioned above to the copyright person system 20 is repeated.

[0074] On the other hand, when a network event is a secrecy contents distribution request (step S200, secrecy contents distribution request), these secrecy contents by which the distribution request was carried out are distributed to the user system 50 (step S220), the response to this secrecy contents distribution request is performed to the user system 50 after that (step S221), and the processing which shifted to step S200 and was mentioned above is repeated. Thereby, secrecy contents can be distributed to the user system 50 from the copyright person system 20 in the secret condition through the contents server 30. In this case, traffic is distributed, and since it is possible to hold secrecy contents to the contents server near the user system 50 beforehand while fast transfer is possible, distribution processing can be processed at a high speed.

[0075] Below, with reference to the flow chart shown in drawing 5 , the internal-processing procedure of a license server 40 is explained. In drawing 5 , a license server 40 judges first whether the network event of a contents use demand was inputted (step S300). when a network event is not inputted (step S300 -- nothing), decision processing of this step S300 is repeated.

[0076] When a network event is a contents use demand (step S300, contents use demand), ACL of the specified contents is searched from the LDAP system 42 (step S301), the access condition related from this searched ACL is extracted further, and new ACL is generated (step 302). When it judges whether there is any correspondence physical element ID certificate corresponding to the physical environmental specification conditions extracted after that (step S303) and there is a correspondence physical element ID certificate (step S303, those with a correspondence physical element ID certificate), as it is When there is no correspondence physical element ID certificate (with step S303 and no correspondence physical element ID certificate) After requiring a certificate from the user system 50 as opposed to the use claimant of contents (step S304), it judges further whether there are any following physical

environmental specification conditions (step S305).

[0077] when the preparations which shift to step S303 and are certainly equipped with a correspondence physical element ID certificate when there are the following physical environmental specification conditions (step S305 -- it is) are made and there are no following physical environmental specification conditions (step S305 -- nothing), a physical element ID certificate group is received (step S306)., the use claimant 50, i.e., the user system, of contents

[0078] Then, license authorization / generation section 41 searches the specified contents decode key (step S307), and re(step S308) arranges the access condition in ACL in the certificate of the physical element which can be forced. Furthermore, processing which bundles all the AND/OR types in ACL with an authentication priority in a parenthesis is performed (step S309). License authorization / generation section 41 performs after that license generation processing which generates a license based on the AND/OR type bundled with this parenthesis (step S310). And the generated license is transmitted to the user system 50 (step S311), and the processing which shifted to step S300 and was mentioned above is repeated.

[0079] Here, the relation of the license and secrecy contents which were generated is explained with reference to drawing 6 . Drawing 6 shows relation with the secrecy contents transmitted to the user system 50 from the copyright person system 20 through the license and the contents server 30 which are transmitted to the user system 50 from a license server 40.

[0080] In drawing 6 , the system ACL 43-1 to 43-5 matched with each secrecy contents 71-75, respectively is stored in ACL43 of a license server 40. The licenses 84-86 over the secrecy contents 71-73 are generated based on this system ACL from the system ACL corresponding to the after that, for example, secrecy, contents 71-73, and it is transmitted to a user system. These licenses 84-86 are enciphered with the corresponding physical element ID, and information does not leak outside. The user system 50 can decode clients 81-ACL 83 from licenses 84-86, can decode secrecy contents 71' corresponding to these - 73', and can obtain contents, respectively.

[0081] In this case, since secrecy contents are also enciphered, security is enough. Thus, ACL and secrecy contents are matched although the transfer roots differ, respectively, maintaining the secrecy condition. In addition, the condition of the secrecy contents sent through the transfer path containing the contents server 30 is expressed as a virtual storing field 70.

[0082] Here, the LDAP system 42 in a license server 40 is further explained with reference to drawing 7 . In drawing 7 , the LDAP system 42 has two or more LDAP

servers, a license server 40 will be positioned as the client-server, and each LDAP server will function on the basis of management of a license server 40. A LDAP server is a directory server using the protocol of the lightweight version of DAP contained in X.500 which is the criterion of a directory service. It has the class of the XML information which was divided by two or more classes in the LDAP server, for example, was described by the individual humanity news 91, the system class 92, MEDIAKURASU 93, and XML.

[0083] And if "own system" is searched in the class of the individual humanity news 91, this system is searched by "system name" from the system class 92, and the present media in the system class 92 "current media" can search MEDIAKURASU 93 out of MEDIAKURASU, and can retrieve the XML information 94 corresponding to these contents from the contents in this MEDIAKURASU 93 further, for example. The information about contents is stored in this XML information 94.

[0084] By the way, the specific use environment of the user system 50 has the logical structure with the layer shown in drawing 8 . In drawing 8 , the specific use environment 100 consists of three layers of the application layer 110, OS kernel layer 111, and the device layer 112, and it connects between each class with the service interface shown by the dotted line. The application layer 110 has contents playback / activation application 101, and has the secret contents decode protection library 102 as a program module inside.

[0085] The secret contents decode protection library 102 operates the storage driver 103, a file system 105, two or more use environmental specification physical element drivers 106-108, and a playback device driver. The storage driver 103 makes a contents storage device drive, the use environmental specification physical element drivers 106-108 make the use environmental specification physical elements 109-111 drive, respectively, and the playback device driver 112 makes the playback device 113 drive. In addition, it may be one physical unit or two roles, the contents storage device 104 and the use environmental specification element 109, may be borne, for example like MO equipment.

[0086] Drawing 9 shows the correspondence relation between OS kernel layer 111 of a use environmental specification physical element (PCSUE), and the device layer 112. As shown in drawing 9 , PCSUE(s) may have inclusion relation. Of course, other devices in the device layer 112 are the same. For example, PCSUE133,134 is positioned by the low order of PCSUE131, and PCSUE135,136 is positioned by the low order of PCSUE134. The data exchange of the information on a physical element ID etc. can be carried out by PCSUE(s) which have such inclusion relation.

[0087] For example, PCSUE of media regenerative apparatus, such as DVD equipment,

includes PCSUE of media, such as DVD, and exchanges contents data and media ID information among both. For example, it is information interchange between PCSUE134 and PCSUE135. And only the top PCSUE performs the data exchange with a PCSUE driver. For example, it is the relation between the PCSUE driver 120 and PCSUE131. Therefore, even if it is the same device layer, it may have inclusion relation and may have hierarchical relation.

[0088] As mentioned above, a license is the consent information over a specific environment, and the access information which becomes the client environment which required the license, i.e., the environment of a user system, from ACL and the content decode key Kc only including the information on a proper is enciphered with a physical element ID (PCSUE-ID).

[0089] Here, it is as follows when an example of the multiplexed license is shown. Namely, [Equation 1]

It comes out. Here, K1 - K5 are PCSUE-ID, respectively. Access information is combined for this license by AND conditions using K1 · K5. It is good for the security reinforcement of a physical element to use each PCSUE-ID for high order, and to encipher in multiplex. The sequential decode of this decryption will be carried out from outside PCSUE-ID at this reverse.

[0090] Moreover, when the security reinforcement of a physical element is almost the same, you may enable it to decode each PCSUE-ID by the code key of the result with EXCLUSIVE OR operation. For example, [Equation 2]

** -- it is good to make it like. The effectiveness of diversification of risks that the danger of the contents decode key Kc theft by attack success to some products, i.e., some physical elements, is distributed by multiplexing of these encryption will be brought about.

[0091] Moreover, [Equation 3] when combining two or more PCSUE-ID by the OR-operation child

** -- when like, it is good also considering the value which generated the sublicense

enciphered by each PCSUE-ID, {< access information >} K1 [for example,], carried out the OR operation of all the sublicenses simply, and was combined as a license. In this case, multiplexing of the encryption mentioned above may be applied also to each sublicense, and you may generate as a license combined with the nest by carrying out AND, XOR, and an OR operation. The effectiveness of diversification of risks is acquired by this.

[0092] Below, the generation procedure of such a license is explained with reference to the flow chart shown in drawing 10 . The flow chart shown in this drawing 10 is the subroutine of the license generation procedure shown in step S310 of drawing 5 . In drawing 5 , it reads from ACL mentioned above 1 word first (step S400). the WORD read after that -- " (" -- it is -- a ****** is judged (step S410).)

[0093] the WORD which carried out reading appearance -- " (" -- it is -- a case (to step S410 and "("), the read-out current position of ACL is memorized as the starting point in [ACL] a parenthesis (step S411).)) Then, Variable NB is set as "0" (step S412), and it reads from ACL 1 word further (step S413). then, the read WORD -- " (" -- it is -- a ****** -- judging (step S414) -- " (" -- it is -- after adding "1" to Variable NB (step S415), it shifts to step S413 and the following 1 word is again read to a case.))

[0094] on the other hand, it judges whether read-out WORD is "" (" -- it is not -- a case (step S414 -- in addition) -- further -- this read WORD -- ") (step S416). When this read WORD is not "", in addition to this, it comes out, and in a certain case, it shifts to step S413 and 1 word is further read from ACL. On the other hand, when this read WORD is "", it judges whether NB is "0" (step S417). When NB is not "0" (steps S417 and NO), "1" subtraction is carried out from the value of NB, and it shifts to step S413, and reads from ACL 1 word further.

[0095] When NB is "0" (steps S417 and YES), the one this side of the current position of ACL is memorized as a terminal point in [ACL] a parenthesis (step S419). Then, license generation processing in [ACL] this parenthesis is performed (step S420), processing which adds the return value by that recursive call to access condition AC is performed (step S421), and it shifts to step S400. ACL in a parenthesis is generated by this.

[0096] the WORD read on the other hand -- " (" -- it is not -- to a case (step S410 -- in addition), it judges further whether this read WORD is physical element conditions or accounting conditions (step S410).) In being physical conditions or accounting conditions, this condition is set as access condition AC (step S431), and it sets up as a secret key Kp of a physical element which can force this condition (step S432), shifts to step S400, and reads from ACL 1 word further.

[0097] When the read WORD is not physical conditions or accounting conditions (step S410, in addition to this), it judges further whether this read WORD is "OR" (step S430). When the read WORD is "OR", license generation processing of next ACL is performed from this read WORD (step S441). Then, when it judges whether AC is contained or not (step S442) and AC is contained in the license generated further (steps S442 and YES), it is set as the license which serves as "{hash [AC,]} Kp and return value" using the return value of the license generation processing by step S441 (step S443), and this generated license is returned (step S454). On the other hand, when AC is not contained in the license (steps S442 and NO), it is set as the license which serves as "{hash [Kc, AC,]} Kp and return value" using the return value of the license generation processing by step S441 (step S445), and this generated license is returned (step S454).

[0098] On the other hand, when the read WORD is not "OR" (step S430, in addition to this), it judges further whether this read WORD is "AND" (step S440). When the read WORD is "AND", license generation processing of next ACL is performed from this read WORD (step S452), and the license which serves as "{hash [a return value, AC,]} Kp" using the return value of this license generation processing is returned (step S454).

[0099] Furthermore, when this read WORD is not "AND" (step S440, in addition to this), the license used as "{hash [Kc, AC,]} Kp" is returned (step S454). Thereby, a license is generated from ACL.

[0100] Below, with reference to the flow chart shown in drawing 11 , the internal-processing procedure of the user system 50 is explained. In drawing 11 , it judges first whether the user system 50 had the use demand of contents (step S500). when there is no use demand of contents (step S500 -- nothing), this decision processing is repeated, and when there is a use demand of contents (step S500 -- it is), the use demand of contents is transmitted (step S501). then, when it judges whether there was any demand of the certificate of a physical element from a license server 40 (step S502) and there is no demand of the certificate of a physical element (step S502 -- nothing), it shifts to step S508.

[0101] on the other hand, when there is a demand of the certificate of a physical element (step S502 -- it is), it judges whether it read (step S503), and the physical element ID certificate was read and went wrong (step S504). When read-out goes wrong (steps S504 and YES), an error notification is transmitted to a license server (step S505), and it shifts to step S500. when it judges whether there is any following physical element on the other hand when read-out does not go wrong (steps S504 and NO) (step S506) and there is the following physical element (step S506 -- it is), it shifts to step S503 and the processing which read the following physical element ID certificate and was mentioned

above is repeated.

[0102] on the other hand, when there is no following physical element (step S506 -- nothing), a physical element ID certificate group is transmitted to a license server 40 (step S507), and receiving contents judge an error or a license further (step S508). The processing which shifted to step S500 and was mentioned above when receiving contents were errors (step S508, error) is repeated, and when receiving contents are licenses (step S508, license), the processing which shifted and mentioned the license above to the physical element (PCSUE) 1 at delivery (step S509) and step S500 is repeated further. Thereby, the user system 50 can acquire a license from a license server 40.

[0103] Here, PCSUE1 shows PCSUE of the beginning of PCSUE of an individual (N-1), generally PCSUEi shows, and i is 1 - (N-1) an integer. Then, an internal-processing procedure when a license is passed to each PCSUEi is explained with reference to the flow chart of drawing 12 .

[0104] In drawing 12 , PCSUEi decodes the received license by Kpi first (step 600). Then, this decoded access condition ACi is evaluated (step S601), and it judges whether it is improper whether the evaluation result of an access condition ACi is good (step S602). When the evaluation result of an access condition ACi is improper (step S602, failure), error processing is performed (step S604) and this processing is ended. On the other hand, when the evaluation result of an access condition ACi is good (step S602, C), this decoded license is transmitted to PCSUE (i+1), decode is continued, and internal processing of Book PCSUEi is ended.

[0105] Next, PCSUE (i+1) is equivalent to PCSUE (N), and the physical element of a playback device performs internal processing here, for example. This internal-processing procedure is explained with reference to the flow chart shown in drawing 13 . In drawing 13 , the received license is first decoded by Kpn (step S700). Then, this decoded access condition AC(N) is evaluated (step S701), and it judges whether this evaluation result is good or improper (step S702). When an evaluation result is improper (step S702, failure), error processing will be performed (step S703), this processing will be ended, and secrecy contents can be decoded as a result.

[0106] On the other hand, when the evaluation result of access condition AC(N) is good (step S702, C), a playback device reproduces the contents which decoded secrecy contents (step S704) and were decoded by this decoded Kc (step S705), and this processing is ended.

[0107] Here, decode processing of a concrete license is explained with reference to drawing 14 . In drawing 14 , the license generated by the license server 40 enciphers

access control list ACL and a contents decode key using the key Kp which is the physical element ID of the playback device 144, and the value of the exclusive OR of DSN141 which is the device serial number of a storage device, and MSN143 which is the media serial number of media 142 is further enciphered as a key.

[0108] First, if write a storage device 140 in media 142, it reads improper MSN, the exclusive OR of this value and DSN of storage device 140 self is calculated and a license is decoded by this result of an operation, a license will serve as {ACL, Kc} Kp. When satisfying the access condition which this license decoded in part is sent to the playback device 144, and the playback device 144 decodes a license using the key Kp which is the physical element ID which playback device 144 self has, acquires the access condition list ACL and the contents decode key Kc, and access condition ACL shows, the contents which could decode and were decoded by the contents decode key Kc will be reproduced by the playback device 144.

[0109] With reference to the data flow which shows the contents decode processing by the license demand and license acquisition which were mentioned above to drawing 15 , it explains further. It sets to drawing 15 , and in the decode protected area in the user system 50, in order to use contents first, a physical element ID certificate is attached and the license demand processing 152 is sent out to a license server 40. Under the present circumstances, a physical element ID certificate is acquired from the use environmental specification physical element 150 by the use environmental specification physical element certification dictation profit processing 153, and is passed by the license demand processing 152.

[0110] On the other hand, if a license is transmitted from a license server 40, the license acquisition processing 156 acquires this license, in access-permission processing 155, while acquiring a license from the license income processing 156, a physical element ID will be acquired through the use environmental specification physical element certification dictation profit processing 153, a use situation will be further acquired from accounting 157, and the use environmental specification physical element ID authentication processing 154 will take [processing] out a decode key using these.

[0111] And the contents decode processing 159 decodes the secrecy contents 158 using a contents decode key, and outputs the contents of a plaintext. In addition, accounting 157 is notified to the use situation monitor physical element 151, and the decrement of the current use situation is automatically carried out according to use with the use environment-monitoring physical element 151.

[0112] By the way, drawing 16 is drawing showing the effect of the protection reinforcement on [at the time of mounting each processing procedure in each entity of

the specific use environment shown in drawing 8]. From this result, generation of a use environmental specification physical element possession certificate is mounted in a device layer, and understands that it is desirable to mount in the device layer by the IC card for accounting information protection. Thus, since protection reinforcement changes also with layers which mount each processing procedure, it is necessary to mount each processing facility which also takes layer arrangement into consideration and is shown in drawing 15 .

[0113] In addition, although the gestalt of operation mentioned above explained as a configuration on the basis of the so-called contents cache possible mold model, it is clear that it is applicable not only to this but the configuration on the basis of a contents coincidence distribution mold model. In this case, the contents server 30 should just deal with it as a configuration by which internal arrangement was carried out into the license server 40.

[0114] Furthermore, what is necessary is to be able to carry either out and just to apply a respectively suitable method according to an adapted system, even if it uses a private key cryptosystem and uses a public key cryptosystem in this case although it is the requisite about encryption and a decryption to use a key with the gestalt of operation mentioned above.

[0115] Moreover, the record medium of portable molds, such as the media used in case not only the equipment of immobilization but this user system 50 is used for the user system 50, i.e., CD-ROM, DVD and MO, an IC card, and a floppy disk, is included in the physical element shown in the gestalt of operation mentioned above. In the user system by which this portable type of record medium is used, in addition to the physical element of immobilization to this user system, this portable type used of record medium will also be contained in a physical element, and use control of contents will be made. In addition, it cannot be overemphasized that it is contained in the physical element which the media of immobilization to the user system 50, for example, the hard disk drive unit of immobilization, ROM of immobilization, etc., mentioned above.

[0116]

[Effect of the Invention] As explained above, according to invention concerning claim 1, a setting means Further two or more partial use authorization conditions of receiving said contents based on the identification information about the physical element of the user means containing the media used within said user means concerned, and the identification information about said user with the combination of an OR and an AND It sets up as use authorization conditions which carried out the structuring expression. Said use control means Since use of said contents by said user means is controlled based

on the use authorization conditions set up by said setting means and it is made to enable flexible use control based on use authorization conditions The effectiveness that flexible contents use control based on this use authorization condition can be performed is done so.

[0117] moreover -- according to invention concerning claim 2 -- a setting means -- since he is trying for the partial use authorization conditions set up to include the accounting conditions which are conditions over the category which changes according to said user means and said user's use situation, they do so the effectiveness that contents use control to a user can be performed further finely and flexibly.

[0118] Moreover, according to invention concerning claim 3, a generation means receives the contents use demand from said user means. The consent information enciphered by the identification information about two or more physical elements of the user means containing the media which use said use authorization conditions and the decode key of said contents within said user means concerned is generated. Said user means decodes said consent information sent according to said contents use demand based on the identification information of the physical element by the user means concerned. Since the decode key of said contents is used and it is made to decode said enciphered contents when satisfying said use authorization conditions, the effectiveness that contents use control with high protection reinforcement can be performed is done so.

[0119] Moreover, since according to invention concerning claim 4 encryption by the identification information of the physical element corresponding to the partial use authorization conditions concerned is multiplexed and is performed when between the partial use authorization conditions within a use authorization condition is described by the AND, the effectiveness that the danger of the theft of the contents decode key by attack success to some physical elements can be distributed is done so.

[0120] Moreover, since according to invention concerning claim 5 it is dealt with as one physical element even if a physical element is a physical element in inclusion relation, the injustice of this one physical element is not allowed, either, but the effectiveness that the danger of calling it the theft of a contents decode key can be distributed is done so.

[0121] Moreover, since it has the contents server which holds the contents enciphered with said information offer authority person means, receives the contents distribution request from said user means, and sends said enciphered contents to the user means concerned on an open network according to invention concerning claim 6, an open network is fully utilized, the congestion of the traffic in the system concerned is prevented, and the effectiveness that contents can be gained quickly is done so.

[0122] According to invention concerning claim 7, moreover, a setting means Further two or more partial use authorization conditions of receiving said contents based on the identification information about the physical element of the user means containing the media used within a user means concerned, and the identification information about said user with the combination of an OR and an AND While setting up beforehand by storing in the condition storing means within said use control means the use authorization conditions which carried out the structuring expression, the decode key of said contents is held for a maintenance means. An extract means receives the use demand of the contents from said user means, extracts the use authorization conditions corresponding to the user means concerned, and the decode key of said contents, generates the consent information which enciphered said use authorization conditions and the decode key of said contents based on the identification information of the physical element sent from said user means, and sends it out to the user means concerned. Since a user means decodes said consent information sent according to said contents use demand based on the identification information of the physical element by the user means concerned, and the decode key of said contents is used and it is made to decode said enciphered contents when satisfying said use authorization conditions, the effectiveness that the encryption and the decryption accompanying flexible contents use control are concretely realizable is done so.

[0123] Moreover, according to invention concerning claims 8 and 9, a demand means accepts the use demand of contents. If the identification information about the physical element of the contents use equipment concerned and the identification information about a user are transmitted to the contents management equipment which manages contents then, from the consent information transmitted by contents management equipment corresponding to the use demand of said contents Decode based on the identification information about the physical element of the contents use equipment concerned, and it asks for use authorization conditions and the decode key of contents. Since said decode key for which it asked is used and it is made to decode contents when said use authorization conditions searched for are judged and a permission is granted, the effectiveness that contents use control with high protection reinforcement can be performed is done so.

[0124] Moreover, according to invention concerning claims 10 and 11, it corresponds to the use demand of contents first, Since it asks for use authorization conditions and the decode key of contents, it decodes from the consent information on contents based on the identification information about the physical element of the contents use equipment concerned, said decode key for which it asked is used when said use authorization

conditions searched for are judged after that and a permission is granted, and it is made to decode about contents, the effectiveness that the contents use control with still higher protection reinforcement can be carried out is done so.

[Brief Description of the Drawings]

[Drawing 1] It is drawing showing the configuration of the contents use control system which is the gestalt of 1 operation of this invention.

[Drawing 2] It is the flow chart which shows the internal-processing procedure of the copyright person system 20 shown in drawing 1 .

[Drawing 3] It is drawing showing an example of accounting conditions and physical environmental specification element conditions.

[Drawing 4] It is the flow chart which shows the internal-processing procedure of the contents server 30 shown in drawing 1 .

[Drawing 5] It is the flow chart which shows the internal-processing procedure of a license server 40 shown in drawing 1 .

[Drawing 6] It is drawing showing relation with the secrecy contents sent from the license and the copyright person system 10 which are sent from a license server 40, or the contents server 30.

[Drawing 7] It is drawing showing the configuration of the LDAP system 42 shown in drawing 1 .

[Drawing 8] It is drawing showing the layer logical structure of a specific use environment.

[Drawing 9] It is drawing showing an example of a physical element with inclusion relation.

[Drawing 10] It is the detail flowchart which shows license generation procedure.

[Drawing 11] It is the flow chart which shows the internal-processing procedure of the user system 50 shown in drawing 1 .

[Drawing 12] It is the flow chart which shows the license decode procedure by the use relation specification physical element.

[Drawing 13] It is the flow chart which shows the license decode procedure by the physical element of a playback device.

[Drawing 14] It is drawing showing an example of the decode process of a license.

[Drawing 15] It is the data flow diagram showing the contents decode processing by a license demand and license acquisition.

[Drawing 16] It is drawing showing the effect of the protection reinforcement on [at the time of mounting each processing procedure in each entity of a specific use

environment].

[Drawing 17] It is drawing showing the access-control model in the former.

[Drawing 18] It is drawing showing the outline configuration of the contents use control system corresponding to the access-control model in the former.

[Drawing 19] It is drawing showing the improved access-control model.

[Drawing 20] It is drawing showing the contents distribution model of the contents use control system in the former.

[Drawing 21] It is drawing showing a contents cache possible mold model.

[Drawing 22] It is drawing showing the outline configuration of the contents use control system corresponding to the contents cache possible mold model shown in drawing 21 .

[Drawing 23] It is drawing showing the outline configuration of the contents use control system which realizes a contents coincidence distribution mold model.

[Description of Notations]

1 Copyright Person

2 User

10 Contents Use Control System

20 Copyright Person System

21 Secret Contents Registration Section

22 Right Transfer Section of Access Control

23 ACL Setting Section

30 Contents Server

40 License Server

41 License Authorization / Generation Section

42 LDAP System

43 Access Control List (ACL)

44 Key

50 User System

51 Secrecy Contents Demand / Acquisition Section

52 License Demand / Acquisition Section

53 Specific Use Environment

54-1 - 54-N Use environmental specification physical element

55-1 - 55-M Contents storage device

56-1 - 56-L Playback device

57-1, 59-1, 61-1 Physical element ID

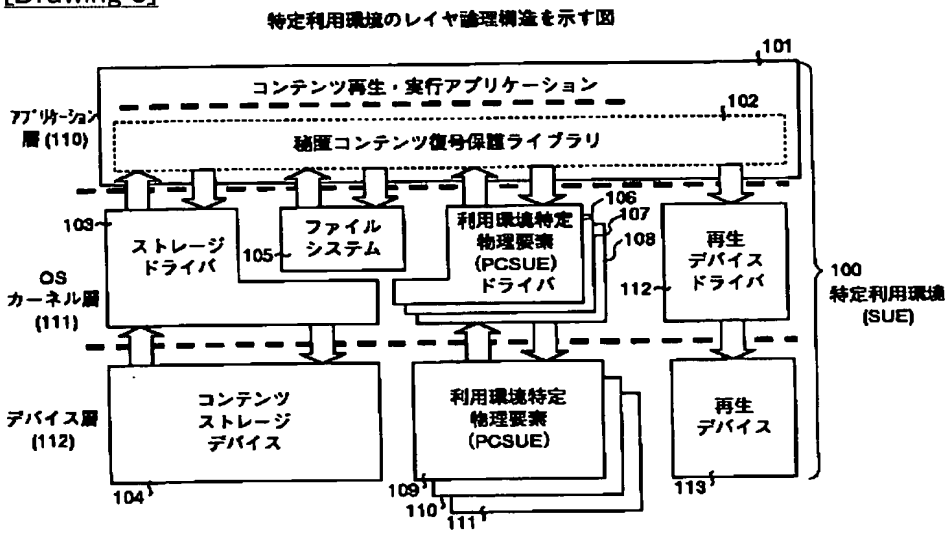
58-1, 60-1, 62-1 Encryption / decryption / evaluation section

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

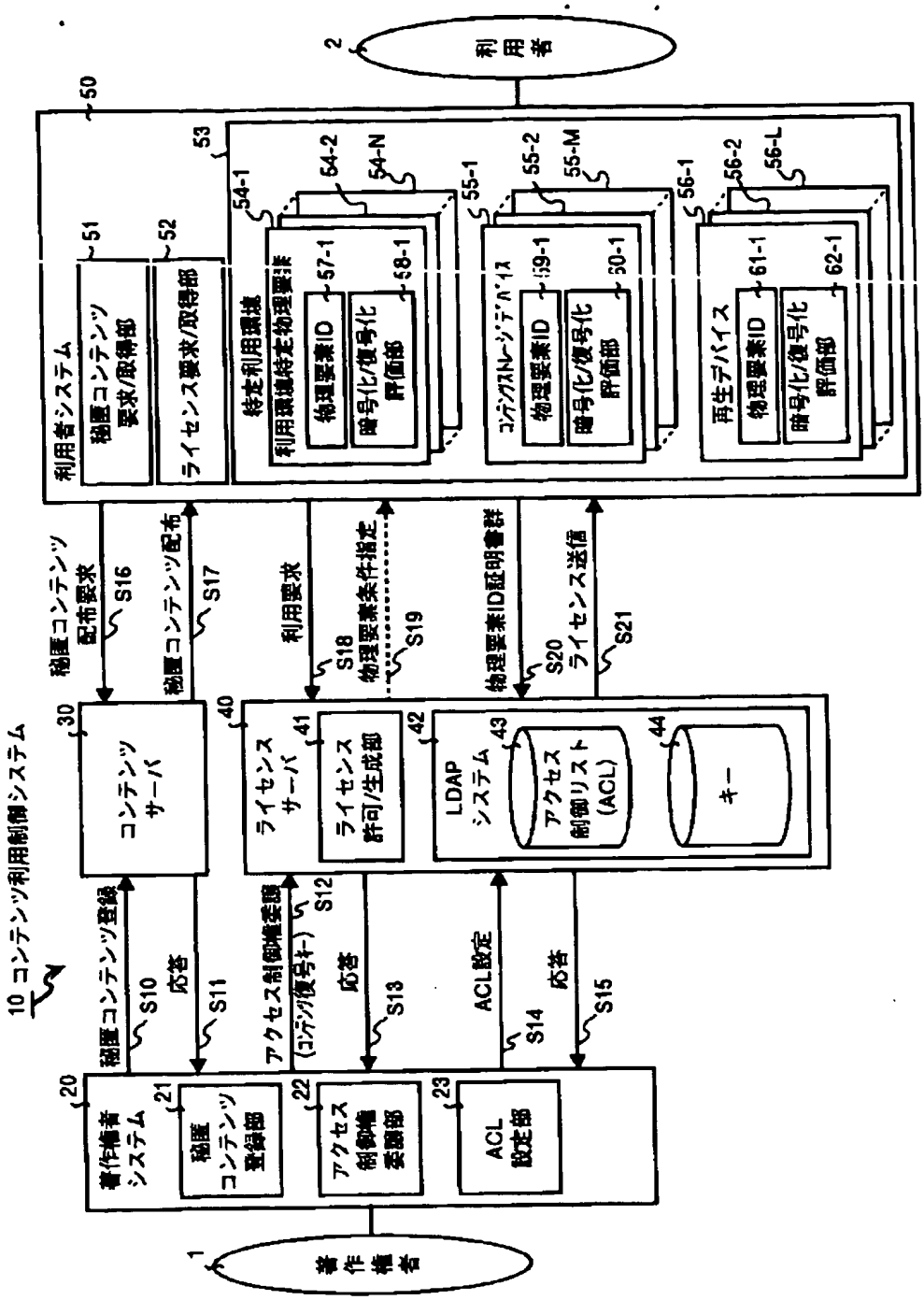
DRAWINGS

[Drawing 8]



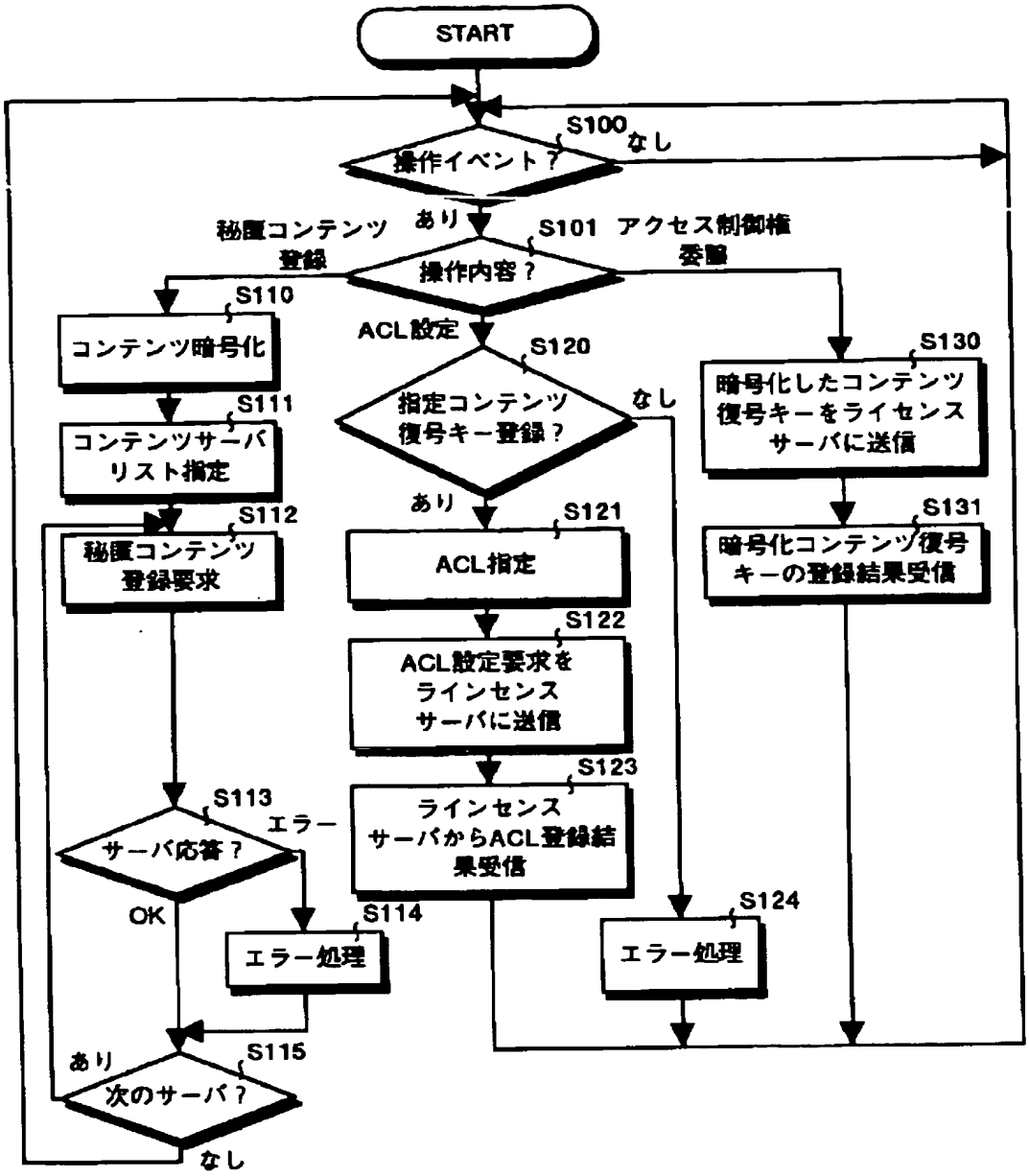
[Drawing 1]

本発明の一実施の形態であるコンテンツ利用制御システムの構成を示す図



[Drawing 2]

図１に示した著作権システム20の内部処理手順を示すフローチャート



[Drawing 3]

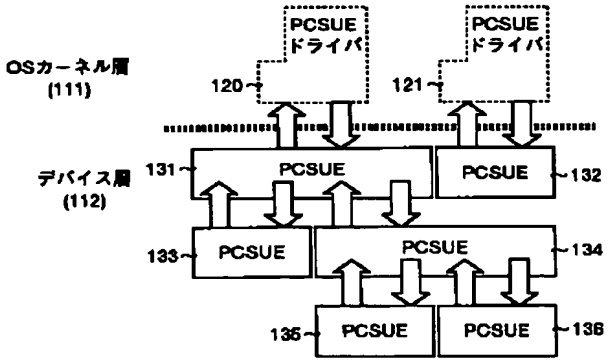
合計条件と物理環境特定要素条件との一例を示す図

会計条件値（Account Condition Value）	利用状況（Usage State）
max Count：操作可能回数最大値	count：操作済回数
max Length：読み出し最大長さ	totalLen：読み出し済長さ＋被要求読み出し長さ
max TimeLen：実行可能最大時間	totalTime：実行済時間長
max Debt：借入可能金額（課金条件）	debt：残金（マイナスは借入金額）

物理環境特定要素（PCSUE）条件	物理要素IDクラス（PCSUE-IDClass）
(1) 計算機本体	PSN (プロセッサシリアル番号)
(2) 周辺デバイス	DSN：デバイスの種別、シリアル番号
(3) メディア	MSN：メディアの種別、シリアル番号
(4) ICカード	certificates：ICカードが発行する証明書
(5) 人体部位（指紋、網膜…）	body Parts：人体部位（指紋、網膜…）認証情報
(6) 許可する時間帯	time Period：時刻（ローカルクロック、GPSなど）
(7) ネットワークドメイン	MACAddress：MACアドレス
(8) 地理的位置（利用国など）	location：GPS/PHS検出位置
(9) 人の記憶	user-ID WithPwd：ユーザIDとパスワード
(10) グループ	group：物理要素IDの集合

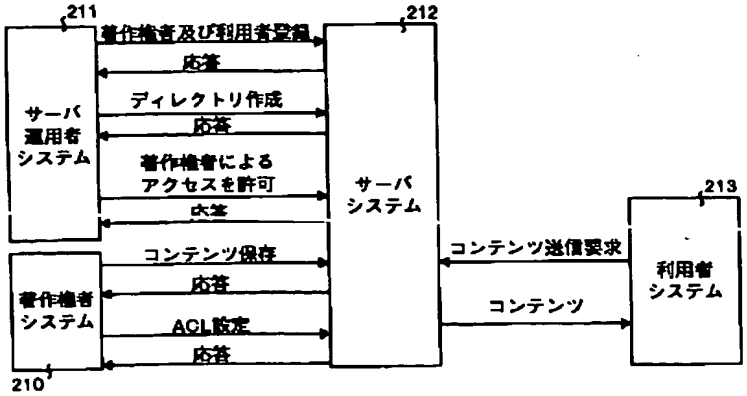
[Drawing 9]

包含関係をもった物理要素の一例を示す図



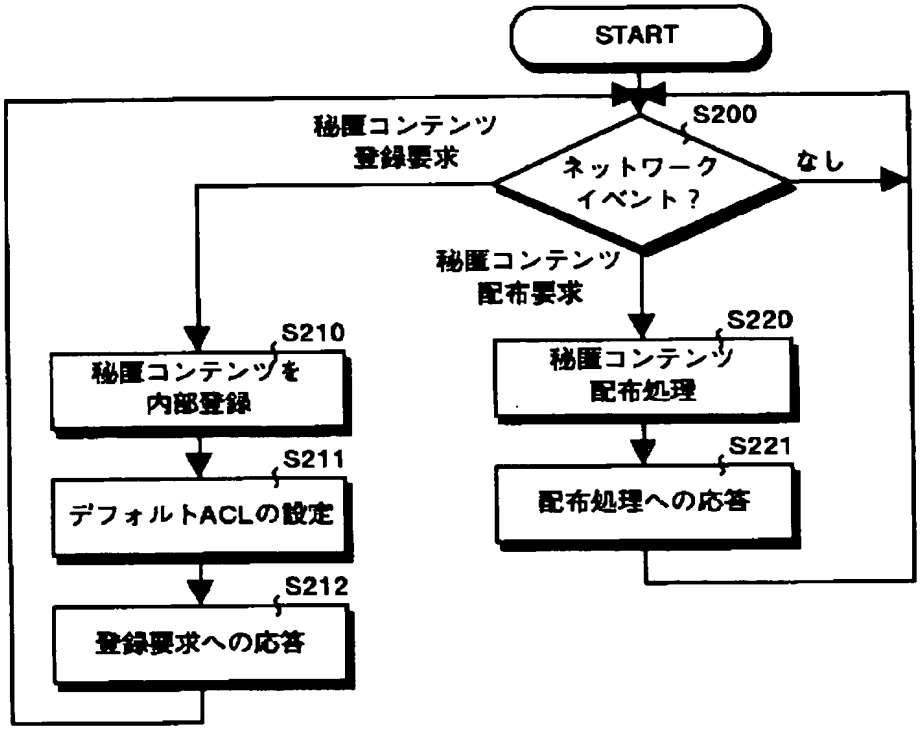
[Drawing 18]

*従来のアクセス制御モデルに対応したコンテンツ利用制御システムの概要構成を示す図



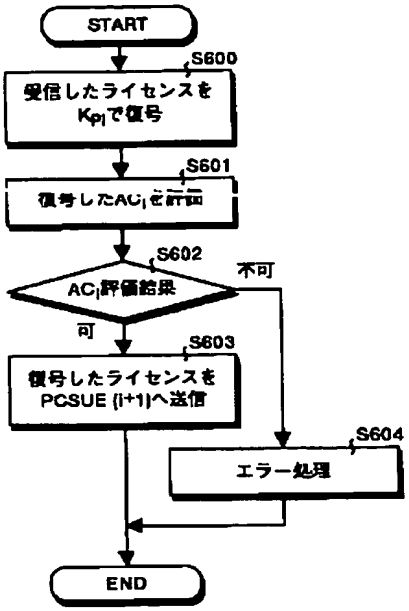
[Drawing 4]

図1に示したコンテンツサーバ30の内部処理手順を示すフローチャート



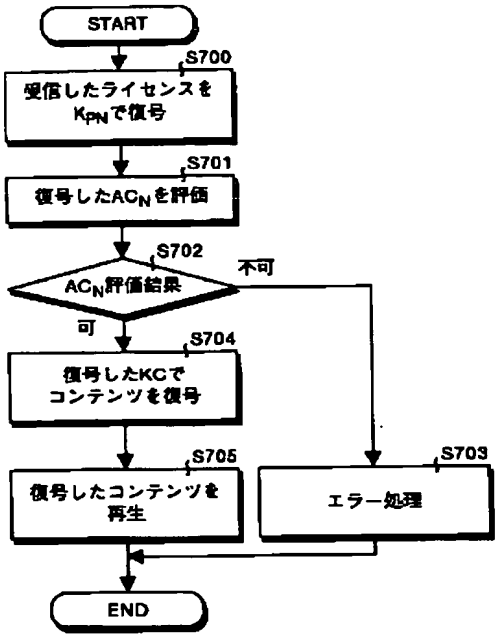
[Drawing 12]

利用者関係特定物理要素によるライセンス復号処理手順を示すフローチャート



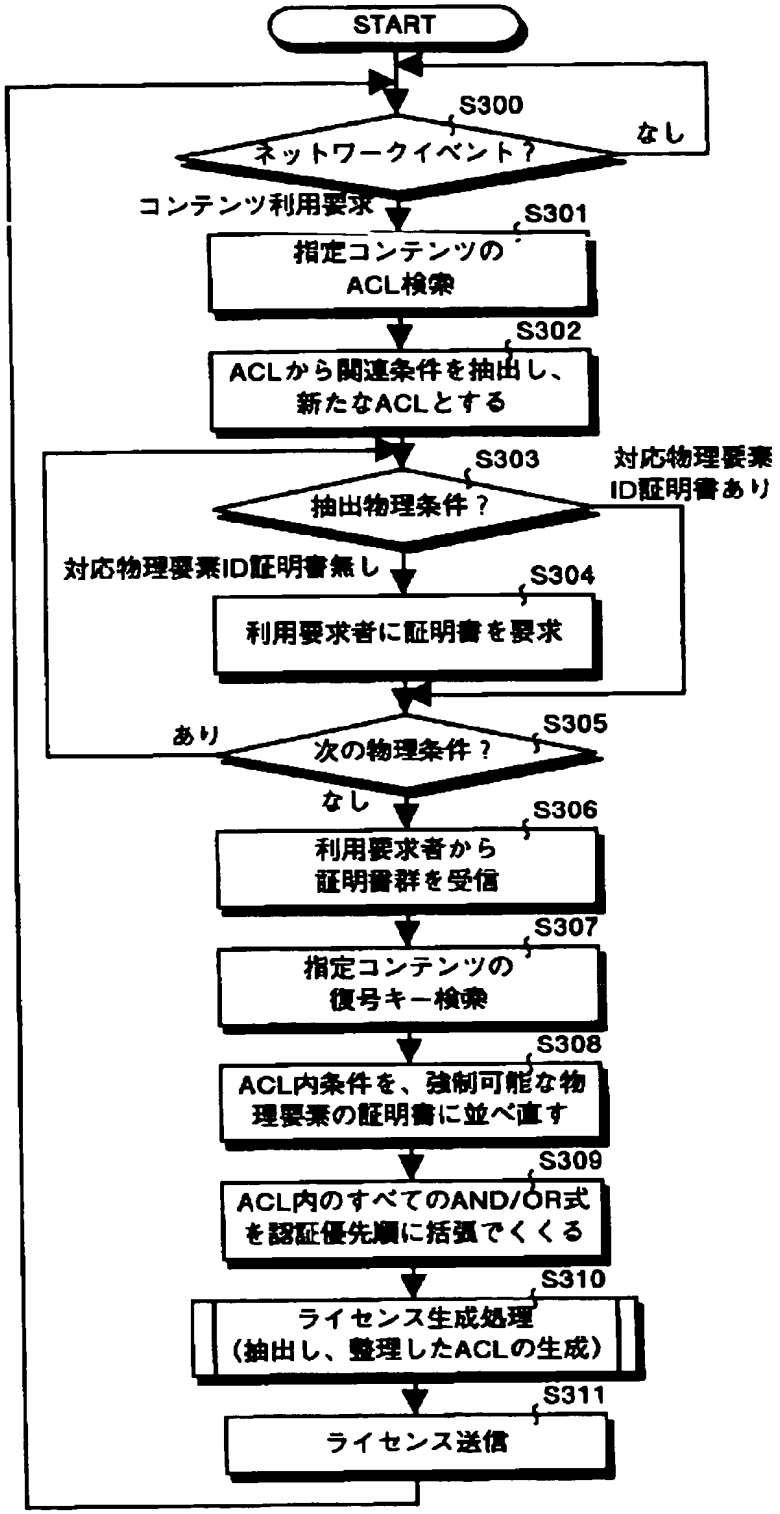
[Drawing 13]

再生デバイスの物理要素によるライセンス復号処理手順を示すフローチャート



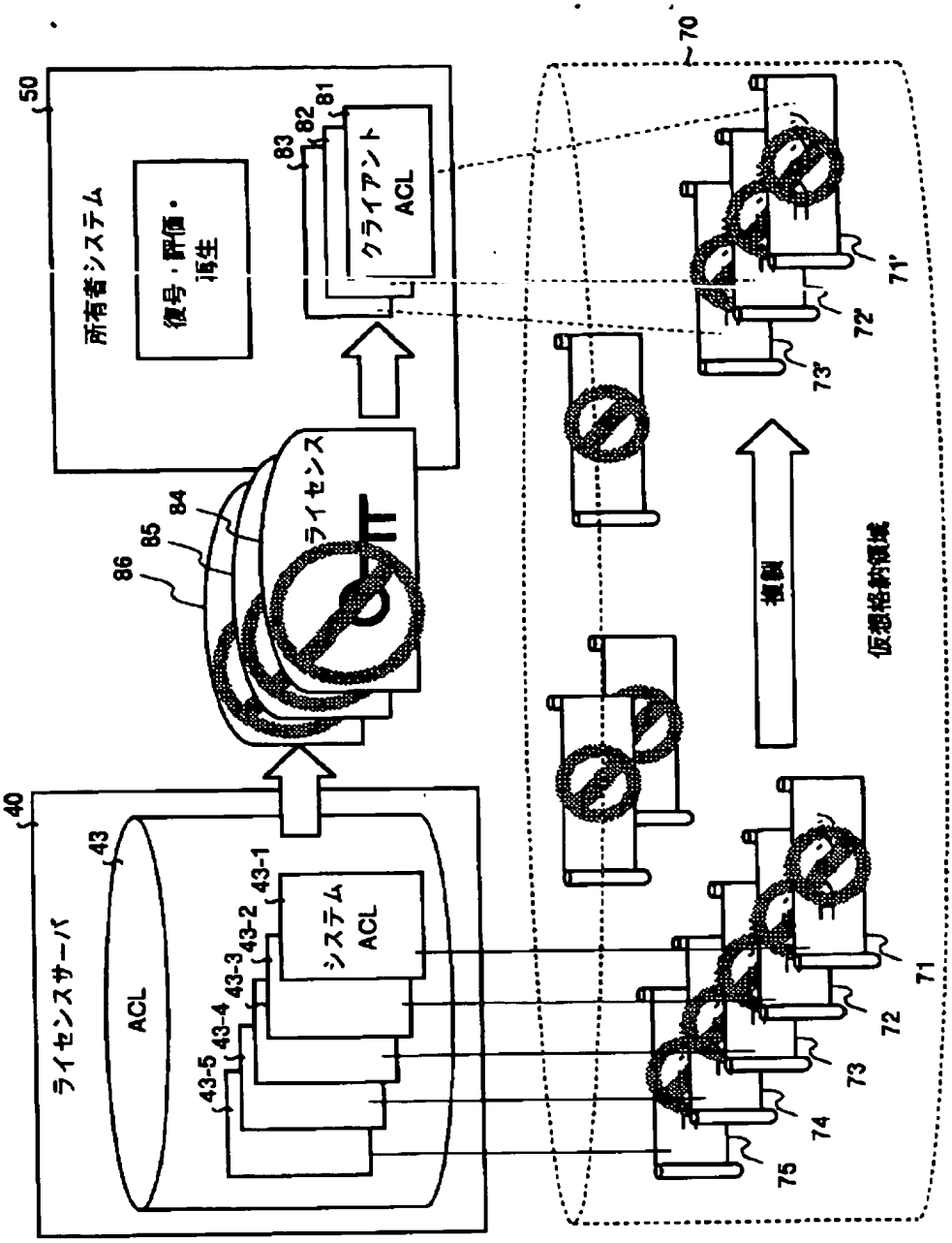
[Drawing 5]

図1に示したライセンスサーバ30の内部処理手順を示すフローチャート



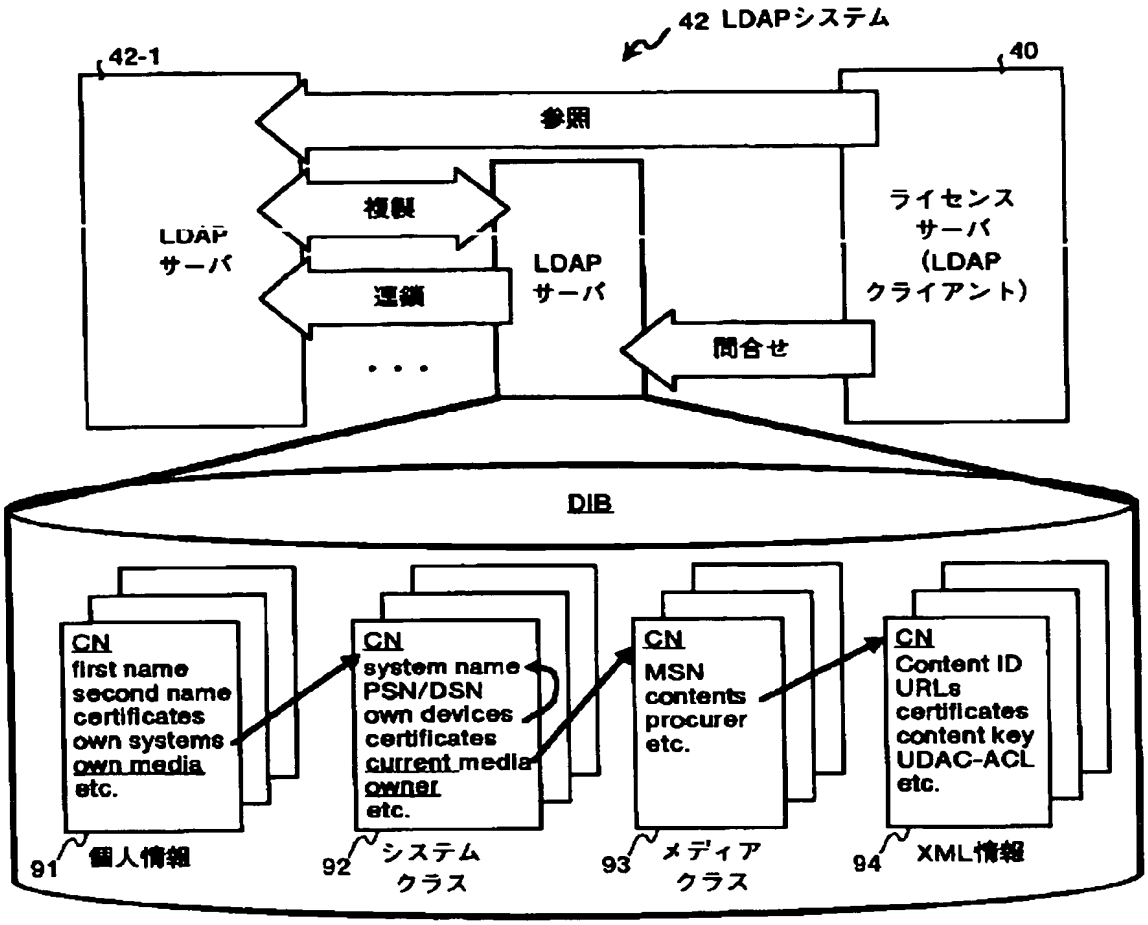
[Drawing 6]

ライセンスサーバ40から送られるライセンスと著作権者システム10あるいは
コンテンツサーバ30から送られる秘匿コンテンツとの関係を示す図



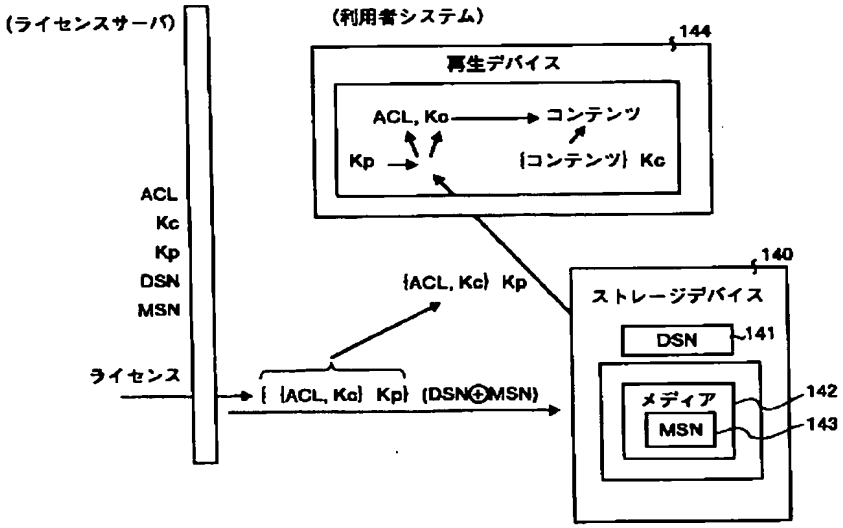
[Drawing 7]

図1に示したLDAPシステム42の構成を示す図



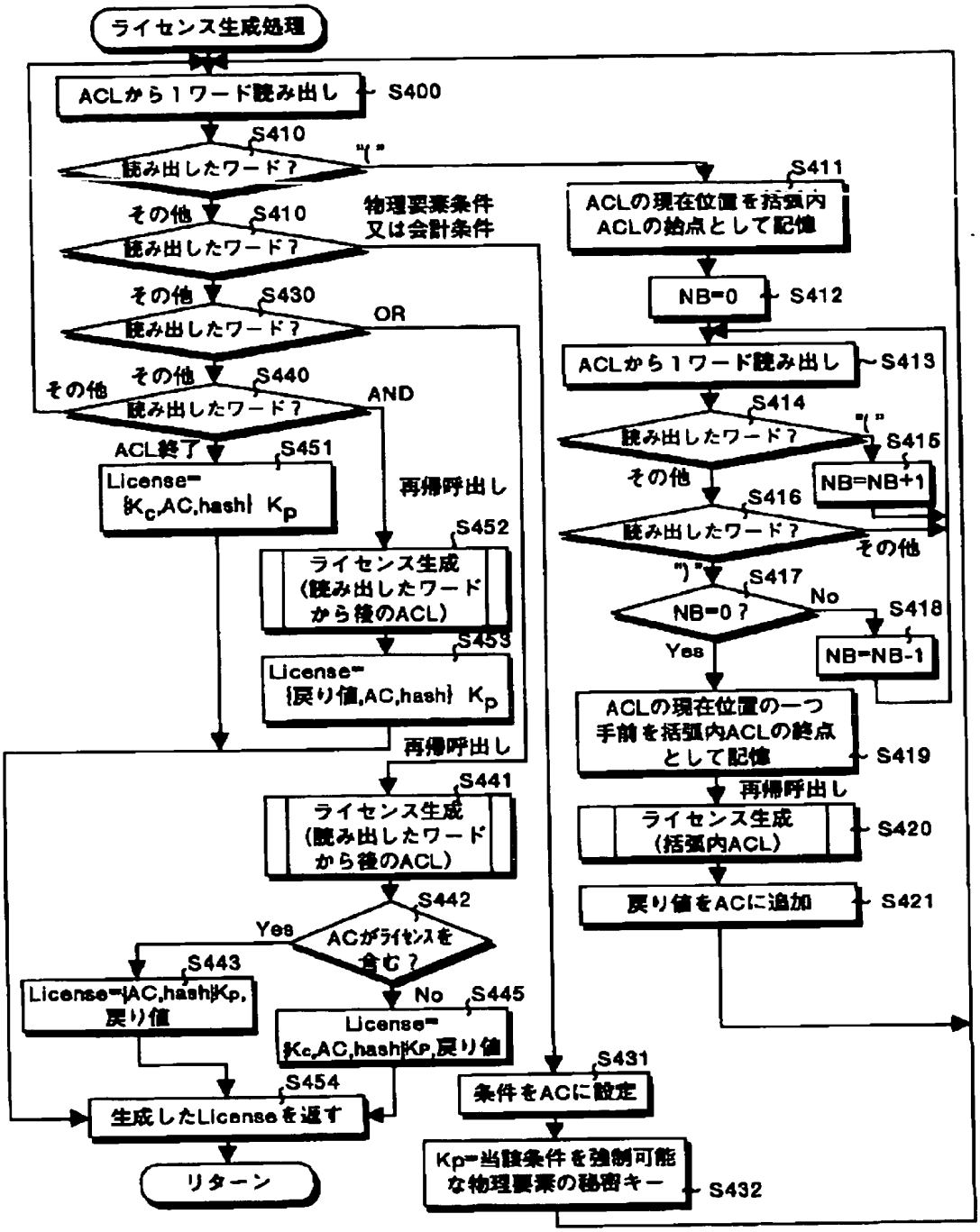
[Drawing 14]

ライセンスの復号課程の一例を示す図



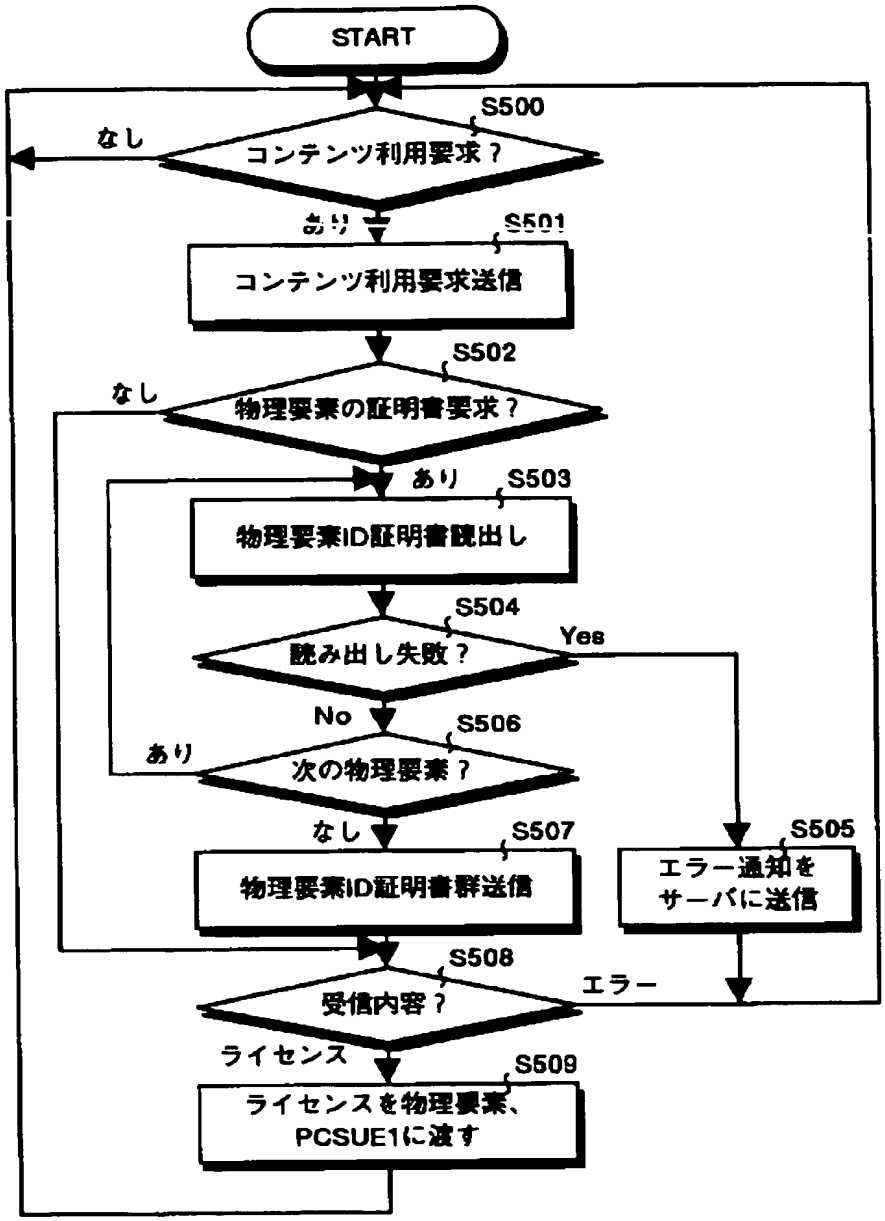
[Drawing 10]

ライセンス生成処理手順を示す詳細フローチャート



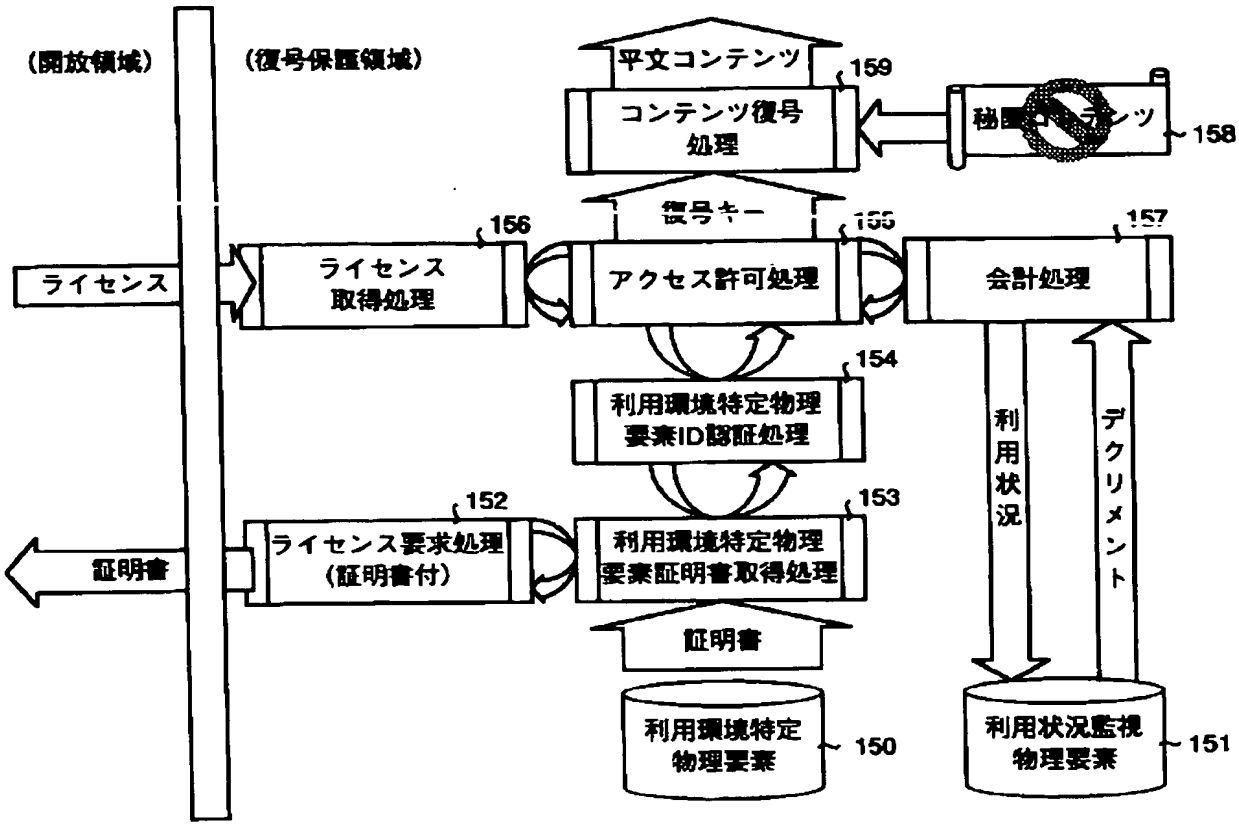
[Drawing 11]

図1に示した利用者システム50の内部処理手順を示すフローチャート



[Drawing 15]

ライセンス要求とライセンス取得によるコンテンツ復号処理を示すデータフロー図



[Drawing 16]

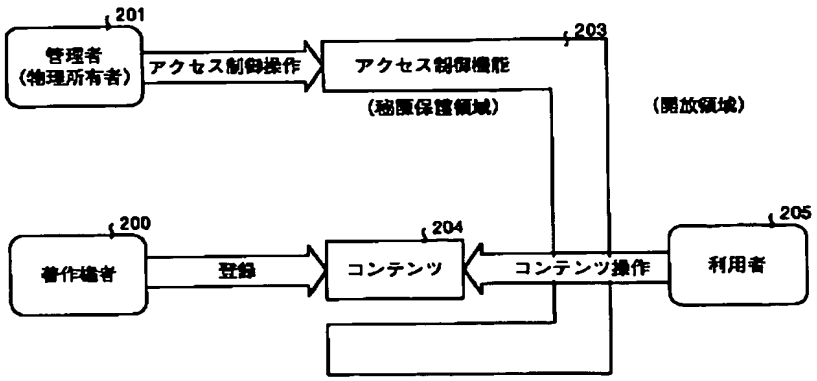
特定利用環境の各エンティティに各処理手続きを実装した場合における保護強度への影響を示す図

	アプリケーション層	デバイスドライバ層	デバイス層
利用環境特定物理要素所有証明書生成	—	○	◎
利用環境特定物理要素ID認証	○	—	—
アクセス制御リスト検索	○	—	○
会計情報保護	△	—	◎ (ICカード)
条件付アクセス許可	○	—	○
復号	○	—	○

—：実装の意義が少ない　△：危険　○：専門家には保護が弱い　◎：保護が強い

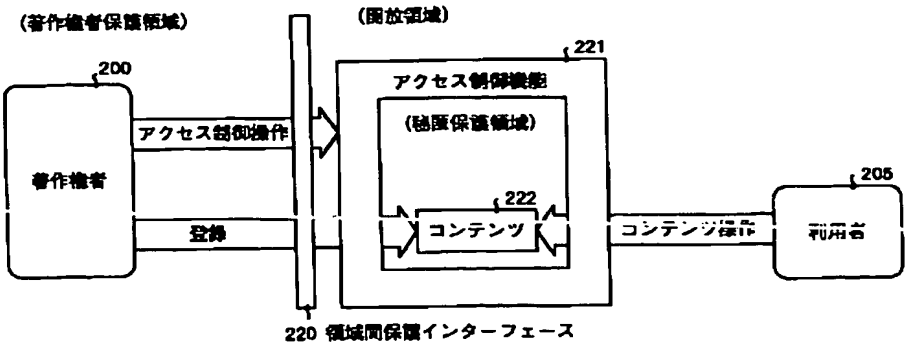
[Drawing 17]

従来のアクセス制御モデルを示す図



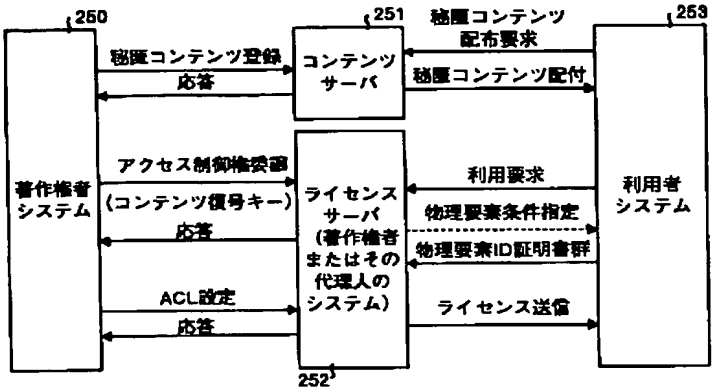
[Drawing 19]

改良したアクセス制御モデルを示す図



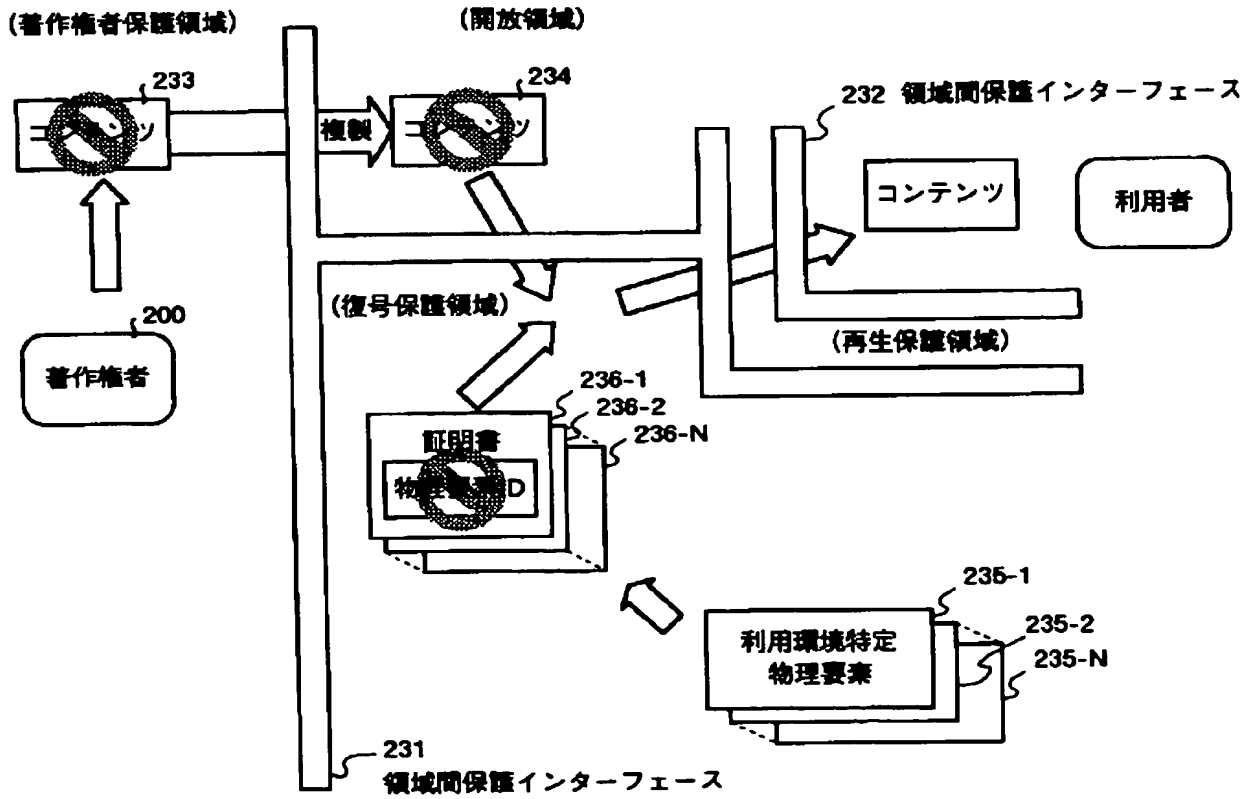
[Drawing 22]

図21に示したコンテンツキャッシュ可能型モデルに対応する
コンテンツ利用制御システムの概要構成を示す図



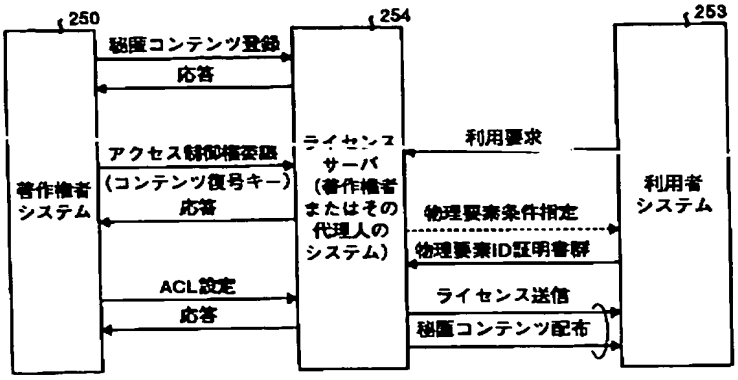
[Drawing 20]

従来のコンテンツ利用制御システムのコンテンツ配布モデルを示す図

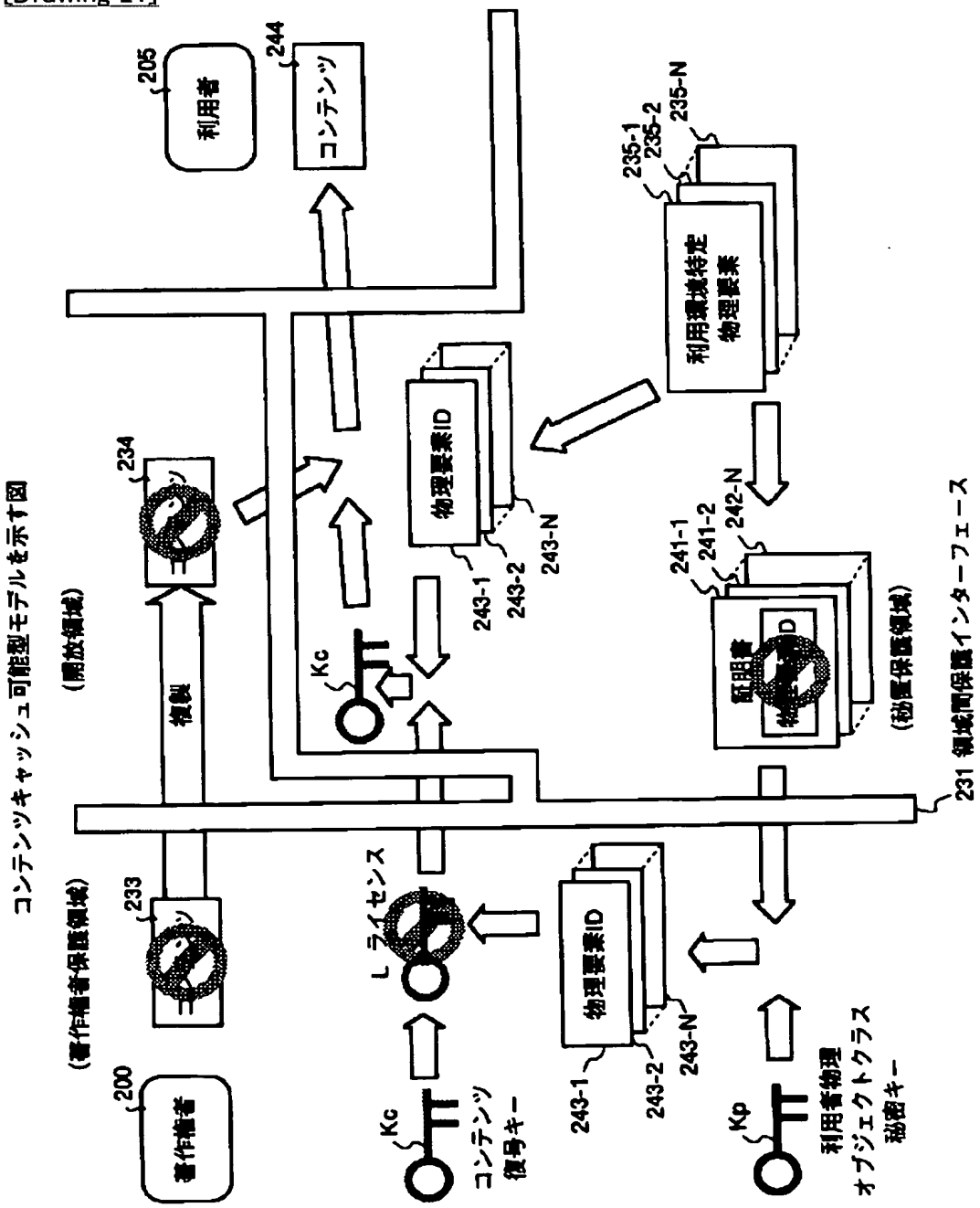


[Drawing 23]

コンテンツ同時配布型モデルを実現するコンテンツ利用制御システムの概要構成を示す図



[Drawing 21]



[Translation done.]